

Bezpečnost v digitálním světě z pohledu pubescentů

Gabriela Klágová

Bakalářská práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta humanitních studií

Univerzita Tomáše Bati ve Zlíně

Fakulta humanitních studií

Ústav pedagogických věd

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Gabriela Klágová
Osobní číslo:	H22312
Studijní program:	B0111A190011 Sociální pedagogika
Forma studia:	Prezenční
Téma práce:	Bezpečnost v digitálním světě z pohledu pubescentů

Zásady pro vypracování

Zpracování rešerše a studium odborné literatury.

Vymezení terminologie a teoretických východisek z oblasti vývojové psychologie – období pubescence, bezpečnosti v digitálním světě a prevence v online prostředí.

Příprava metodiky empirické části, zpracování projektu výzkumu a stanovení výzkumného problému.

Realizace kvantitativního výzkumu formou dotazníku.

Zpracování a vyhodnocení získaných dat, včetně jejich interpretace.

Prezentace výsledků výzkumu, jejich shrnutí a doporučení pro praxi.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

- CHRÁSKA, Miroslav, 2016. Metody pedagogického výzkumu: základy kvantitativního výzkumu. Praha: Grada. ISBN 978-802-4753-263.
- KOŽÍŠEK, Martin a Václav PÍSECKÝ, 2016. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada. ISBN 978-80-247-5595-3.
- LANGMEIER, Josef a Dana KREJČÍŘOVÁ, 2006. Vývojová psychologie. Praha: Grada. ISBN 978-80-247-1284-0.
- ŠMAHEL, David, 2003. Psychologie a internet: děti dospělými, dospělí dětmi. Praha: Triton. ISBN 80-7254-360-1.
- THOROVÁ, Kateřina, 2015. Vývojová psychologie: proměny lidské psychiky od početí po smrt. Praha: Portál. ISBN 978-80-262-0714-6.

Vedoucí bakalářské práce: **Mgr. Eliška Suchánková, Ph.D.**
Ústav pedagogických věd

Datum zadání bakalářské práce: **13. ledna 2025**
Termín odevzdání bakalářské práce: **2. května 2025**

L.S.

Mgr. Libor Marek, Ph.D.
děkan

doc. Mgr. Jakub Hladík, Ph.D.
ředitel ústavu

Ve Zlíně dne 13. ledna 2025

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Tato bakalářská práce se zabývá problematikou bezpečnosti v digitálním světě z pohledu pubescentů ve věku od 11 do 15 let. Digitální technologie výrazně ovlivňují trendy a životní styl mladé generace, a právě pubescenti tvoří velmi zranitelnou skupinu v online prostředí. Cílem práce je prostřednictvím kvantitativního výzkumu, realizovaného formou dotazníkového šetření, zjistit, jaká rizika spojená s tímto tématem pubescenti znají a jak je vnímají. Zkoumá, zda se s některými riziky setkali, jaké emoce v nich tyto situace vyvolaly a jaké preventivní strategie si vůči rizikům vyvinuli. V závěru práce je opakovaně zdůrazněn význam prevence a osvěty, jelikož je v digitálním světě klíčová. Toto téma práce je přínosné především svou aktuálností a komplexním pohledem na rizika digitálního světa.

Klíčová slova: digitální svět, pubescent, bezpečnost na internetu, prevence, kyberšikana, kybergrooming, dezinformace, stalking a kyberstalking, fenomén youtubering, rizikové užívání sociálních sítí

ABSTRACT

This bachelor's thesis examines the issue of safety in the digital world from the perspective of pubescents aged 11 to 15. Digital technologies have a significant impact on the trends and lifestyle of the younger generation, and pubescents constitute a particularly vulnerable group in the online environment. The aim of the thesis is to identify, through quantitative research in the form of a questionnaire survey, which risks associated with this topic pubescents are aware of and how they perceive them. It also explores whether they have encountered certain risks, what emotions these situations evoked, and what preventive strategies they have developed. In the conclusion, the importance of prevention and education is repeatedly emphasized, as these are crucial in the digital world. The topic of this thesis is particularly relevant due to its timeliness and the comprehensive perspective it offers on the risks of the digital world.

Keywords: digital world, pubescent, internet safety, prevention, cyberbullying, cyber grooming, disinformation, stalking and cyberstalking, phenomenon of youtubing, risky use of social networks

Ráda bych poděkovala vedoucí bakalářské práce Mgr. Elišce Suchánkové, Ph.D. za vedení a cenné rady při psaní mé bakalářské práce. Děkuji také všem svým respondentům, za ochotu a čas spojený s vyplněním mého dotazníku. Dále bych chtěla poděkovat své rodině, a to zejména své mamince a příteli za pomoc a podporu během celého studia i psaní této práce.

„Kybernetická bezpečnost je mnohem víc než jen záležitost IT.“ – Stephane Nappo

OBSAH

ÚVOD.....	11
I TEORETICKÁ ČÁST	12
1 PUBESCENCE JAKO OBDOBÍ ADOLESCENCE.....	13
1.1 ADOLESCENCE	13
1.1.1 Raná adolescence – pubescence.....	14
1.1.2 Pozdní adolescence	15
1.2 PUBESCENTI A CHOVÁNÍ NA INTERNETU	16
1.2.1 Agresivní chování	16
1.2.2 Role rodičů	17
1.2.3 Negativní vlivy sociálních sítí.....	17
2 BEZPEČNOST V DIGITÁLNÍM SVĚTĚ.....	18
2.1 KYBERŠIKANA.....	18
2.1.1 Projevy kyberšikany	19
2.1.2 Anonymita.....	20
2.1.3 Krádež identity	20
2.1.4 Šíření citlivých dat	21
2.2 KYBERGROOMING	21
2.2.1 Mirroring	22
2.2.2 Phishing.....	22
2.2.3 Profiling.....	24
2.2.4 Luring.....	25
2.2.5 Sexting.....	25
2.2.6 Izolace oběti	25
2.2.7 Lákání skrze fotografii opačného pohlaví.....	26
2.2.8 Webcam trolling.....	26
2.3 STALKING A KYBERSTALKING	26
2.4 RIZIKOVÉ VYUŽÍVÁNÍ SOCIÁLNÍCH SÍTÍ	28
2.5 DEZINFORMACE	29
2.5.1 Spam.....	29
2.5.2 Hoax	30
2.5.3 Fake news.....	30
2.6 FENOMÉN YOUTUBERING	30
2.7 DŮSLEDKY RIZIK	32
3 PREVENCE A OCHRANA V DIGITÁLNÍM SVĚTĚ.....	33
3.1 DESATERO BEZPEČNÉHO CHOVÁNÍ NA INTERNETU OD E-BEZPEČÍ.....	33
3.1.1 Ochrana osobních údajů	33
3.1.2 Silná a unikátní hesla	33
3.1.3 Dvoufaktorové zabezpečení účtů	34
3.1.4 Opatrnost při internetovém seznamování.....	34

3.1.5	Odesílání intimních fotografií a videí	34
3.1.6	Důvěra	34
3.1.7	Slušné chování a respekt k druhým	35
3.1.8	Podezřelé odkazy a přílohy	35
3.1.9	Opatrnost při online nakupování	35
3.1.10	Žádost o pomoc	36
3.2	ANTIVIROVÉ PROGRAMY	36
3.3	OSVĚTA	36
3.4	POMOC PŘI ŘEŠENÍ VZNIKLÉHO PROBLÉMU	37
3.4.1	Podpora oběti.....	38
3.4.2	Eliminace následků.....	38
3.4.3	Obnovení bezpečnosti	39
II	PRAKTICKÁ ČÁST	40
4	VÝZKUM.....	41
4.1	VÝZKUMNÉ CÍLE.....	42
4.2	VÝZKUMNÉ OTÁZKY	42
4.3	DRUH VÝZKUMU.....	43
4.4	VÝZKUMNÝ SOUBOR	43
4.5	METODA VÝZKUMU	45
4.6	ZPŮSOB ZPRACOVÁNÍ DAT	46
4.7	LIMITY VÝZKUMU.....	46
5	ANALÝZA	47
5.1	JAKÉ TYPY DIGITÁLNÍCH RIZIK JSOU PUBESCENTŮM NEJVÍCE ZNÁMÉ?	47
5.2	JAKÉ JSOU ZKUŠENOSTI PUBESCENTŮ S DIGITÁLNÍMI RIZIKY PŘI UŽÍVÁNÍ ONLINE PROSTŘEDÍ?	49
5.3	JAKÉ JSOU POCITY PUBESCENTŮ PŘI SETKÁNÍ S TĚMITO RIZIKY?.....	61
5.4	JAKÉ STRATEGIE UŽÍVAJÍ PUBESCENTI V PREVENCI RIZIK SPOJENÝCH S POUŽÍVÁNÍM DIGITÁLNÍCH TECHNOLOGIÍ?	68
6	SHRNUTÍ VÝSLEDKŮ A INTERPRETACE DAT.....	74
	ZÁVĚR.....	78
	SEZNAM POUŽITÉ LITERATURY	79
	SEZNAM OBRÁZKŮ	89
	SEZNAM TABULEK.....	90
	SEZNAM GRAFŮ	91
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	92
	SEZNAM PŘÍLOH.....	93

ÚVOD

Současná generace vyrůstá ve společnosti, kde jsou moderní technologie každodenní součástí života. Internet, chytré telefony a sociální sítě se staly hlavním prostředkem komunikace, sdílení informací i trávení volného času. Ač se může zdát, že moderní technologie otevírají ideální svět plný možností, realita s sebou nese i stinné stránky. Spolu s výhodami, jako je snadný a rychlý přístup k informacím a neustálé propojení s okolím, se objevují i rizika, která bývají často podceňována. Důležité je zejména věnovat se této problematice u dětí v období pubescence, u kterých se teprve formují digitální návyky a jejich schopnost kritického myšlení není dostatečně vyvinuta.

Pozornost této bakalářské práce je zaměřena právě na pubescenty a jejich pohled na bezpečnost v digitálním světě. Cílem je zjistit, jak mladí uživatelé vnímají rizika spojená s využíváním digitálních technologií a jak se v online prostředí chovají. Jejich přístup a způsob chování má pak přímý vliv na to, s jakými formami rizik se mohou setkat. Nedostatečná obezřetnost či podcenění závažnosti by v tom mohly hrát zásadní roli.

Teoretická část práce se soustředí na definici pojmů souvisejících s vývojovými specifiky období pubescence a digitální bezpečností. Vývojové období pubescence je popsáno včetně jeho charakteristik a specifik, kromě toho také jejich chování v prostředí internetu. Klíčovým východiskem je typologie rizik vycházející z projektu E-bezpečí, který se dlouhodobě věnuje prevenci a osvětě digitální bezpečnosti. Díky ní tato práce poskytuje komplexní pohled na různé typy rizik, od kyberšikany, přes sexting až po fenomén youtubering. V závěru teoretické části jsou také shrnuta doporučená preventivní opatření, jak se proti těmto rizikům chránit, a jak popřípadě obnovit ochranu po útoku.

Praktická část navazuje na teoretický rámec a věnuje se výzkumu, jeho analýze a prezentaci výsledků, přičemž jsou mezi odpověďmi hledány souvislosti mezi pohledem na chování pubescentů, popřípadě jejich preventivní opatření, a skutečnými zkušenostmi. Výsledky výzkumu jsou zasazeny do kontextu dosavadních výzkumů a odborné literatury. V případě rozdílů mezi výsledky této práce a studiemi jiných autorů je navržena možná příčina těchto rozdílů.

Cílem je přispět k většímu porozumění chování pubescentů v digitálním prostředí. Výsledky mohou nabídnout náhled do současných trendů v chování mladistvých a posloužit jako podklad nebo inspirace pro další výzkumy i pro tvorbu preventivních aktivit, které by podpořily bezpečnější pohyb dětí i dospívajících v digitálním prostředí.

I TEORETICKÁ ČÁST

1 PUBESCENCE JAKO OBDOBÍ ADOLESCENCE

Lidský život je vývojovými psychology rozdělován do takzvaných vývojových etap. Každá z těchto etap je charakteristická svými změnami v organismu, které jsou ovšem individuální pro každého jedince. Tyto etapy jsou vymezeny hranicemi, mají přesně dané pořadí, dobu trvání i svá specifika a projevy (Thorová, 2015).

Tato kapitola je zaměřena na etapu pubescence, kterou lze považovat za specifickou fázi v rámci adolescence. Nejdříve je ale potřeba obecně definovat adolescenci z komplexního pohledu.

1.1 Adolescence

Období dospívání je charakterizováno jako přechodná fáze mezi dětstvím a dospělostí, přičemž je dle Vágnerové (2021) vymezen přibližně od 10. až 20. roku života. Během této životní etapy dochází k rozsáhlým proměnám osobnosti, které se projevují v rovině tělesné, psychické i sociální. Ty jsou ovlivněny biologickými faktory, ale jejich průběh a intenzita jsou výrazně ovlivněny také faktory psychologickými a sociálními. Mimo to je také úzce spjat s kulturním a společenským kontextem.

Thorová (2015) vymezuje adolescenci jako období pozdního dětství, konkrétně od 12/13 do 19 let. Tento vývojový proces začíná nástupem puberty, která se projevuje specifickými tělesnými změnami a zvýšenou produkcí pohlavních hormonů. Kromě toho probíhá také rozvoj emoční, kognitivní a sociální oblasti. V tomto období jsou na jedince kladeny rostoucí sociální požadavky s cílem přípravy na samostatný a zodpovědný život, což může vést ke zvýšené míře stresu, který se může projevit pocitem úzkosti nebo odmítání přechodu do dospělosti. Kromě toho se zvyšuje pravděpodobnost vzniku rizikového chování a psychopatologických procesů.

Rozsah biologických změn je individuální, žáci se ve školním prostředí setkávají s různou mírou a tempem tělesného vývoje spojeného s pubertou. Pedagog by měl s těmito odlišnostmi pracovat, protože jejich opomíjení může vést k rozvoji šikany (Dolejš a Orel, 2017). Kromě pohlavního zrání a dosažení reprodukčních schopností je tato fáze také spojována s emoční nestabilitou a vyspělejším způsobem myšlení, který zahrnuje formálně abstraktní uvažování a dosahování vrcholu jeho rozvoje. Nové sociální zařazení jednotlivce do společnosti s sebou nese určitá očekávání ohledně chování a výkonů, což vede ke změně pojetí vlastní role a přehodnocení sebepojetí. Všechny změny se odehrávají souběžně

a vzájemně se ovlivňují, mimo to ale také dochází k ovlivňování ze stran dalších sociálních, ekonomických a kulturních faktorů a významných osob, jako jsou rodiče, učitelé a další. I přesto ale někteří jedinci neprocházejí pohlavním zráním a už vyspívají v myšlení, přičemž dokáží kriticky hodnotit sebe i ostatní. Jiní zase pohlavně dospívají, ale emoční a intelektuální zralost je na nižší úrovni (Langmeier a Krejčířová, 2006).

1.1.1 Raná adolescence – pubescence

Raná adolescence, známá také jako pubescence, se vymezuje obdobím zhruba od 11 do 15 let života. Největších změn si lze všimnout na tělesné stránce. Změna vzhledu dospívajícího dále ovlivňuje sebepojetí jedince a reakci jeho okolí. Také se ukazují ve způsobu myšlení, kdy pubescenti začínají uvažovat i o hypotetických situacích. Jedinec se začíná odpoutávat od rodičů a stále více se váže na své vrstevníky. Velkou roli hraje přátelství, první lásky a experimentování s partnerskými vztahy. Starší pubescenti se chtějí odlišit od dětí a dospělých, což se projevuje změnami ve vzhledu, životního stylu, hodnotách a zájmech. Mezi klíčové sociální mezníky patří ukončení povinné školní docházky a rozhodování o profesním směřování, což má zásadní vliv na budoucí sociální postavení. Mimo to také pubescent vyžaduje větší svobodu v rozhodování, což však může vést ke snížení pocitu jistoty, který byl zajišťován rodinnou závislostí. Potřeba pocitu jistoty je těsně spjata s potřebou citové akceptace, která je v tomto období velmi zásadní (Vágnerová a Lisá, 2021). Snaha odprosit se od závislosti na rodičích je formou jakési vzpoury, přičemž na konci tohoto období se vztah upevňuje a obnovuje (Thorová, 2015).

Dle Langmeiera a Krejčířové (2006) lze období pubescence dále rozdělit do dvou fází:

- **Fáze prepuberty** – toto období je vyznačováno počátkem pohlavního dospívání, a to zejména objevením sekundárních pohlavních znaků a často rychlým růstem. U dívek trvá tato fáze zhruba od 11 do 13 let, zatímco u chlapců o 1–2 roky později.
- **Fáze vlastní puberty** – následuje po prepubertě a trvá až do dosažení reprodukční schopnosti. U dívek nastane pravidelná menstruace, cyklus a schopnost oplodnění až po nějaké době, přibližně za 1–2 roky. Plná reprodukční způsobilost se u chlapců rozvíjí až v návaznosti s ukončením růstu sekundárních pohlavních znaků.

V komunikaci pubescentů s dospělými (zejména rodiči) často dochází ke vzájemnému nepochopení, zvýšenému napětí a konfliktům. Své chování pubescenti často přizpůsobují, aby nedošlo ke konfliktu a zároveň aby nebyl odhaleno příliš mnoho ze soukromí (pocity i názory). Názory dospělých často nevnímají a mají tendenci je považovat za neaktuální

a opakující se. Dospělí chtějí komunikaci posílit, což může mít opačný efekt (Vágnerová a Lisá, 2021). Dospívající ale k autoritám mají odpor a dochází k odmítání či zpochybňování bez racionálního odůvodnění. Také si lze povšimnout výrazné emoční nestability, která se projevuje častými výkyvy nálad a také odporu vůči autoritám (Kyselá, 2019).

Komunikace s vrstevníky je odlišná a má specifické vzorce, jako jsou oblečení, vlastnictví daných věcí, úprava sebe samého či využívání zkratk (v rámci dané skupiny) a specifických forem oslovení. Komunikace je doprovázena i gestikulací, mimikou, dotyky či dalšími prvky fyzického kontaktu. Vzájemná interakce ve skupině slouží k upevňování pocitu sounáležitosti a vyjádření skupinové identity. Tyto projevy často nemají obsahovou hodnotu, ale slouží k upevnění vztahů, což ale souvisí s adolescentním egocentrismem. Tento kontakt mají potřebu udržovat prostřednictvím dlouhých telefonátů či výměn zpráv s cílem upevnit existující vztahy. Frekvence komunikace bývá dospělými vnímána jako nadměrná a zbytečná, přičemž se snaží jejich čas omezit. Takové chování převládá spíše u dívek než u chlapců. Významnou roli v komunikaci dospívajících hrají také sociální sítě, které umožňují udržení vztahů, ale také možnost sebe prezentace a projevení aktuálních preferencí (Vágnerová a Lisá, 2021).

1.1.2 Pozdní adolescence

Ačkoliv pozdní adolescence není centrem zájmu této práce, pro zasazení do kontextu je třeba definovat i toto období. Dle Langmeiera a Krejčířové (2006) je přibližně ohraničeno věkem od 15 do 22 let. V této fázi dochází k dosažení plné reprodukční zralosti a dokončení tělesného růstu. Přejít ze základní na střední školu (popř. učební obor) přináší rychlé změny v postavení jedince ve společnosti. Dochází ke změně sebepojetí a také počátku erotických vztahů.

Dochází také k rozsáhlým psychosociálním změnám, které ovlivňují utváření osobnosti a sociálního postavení jedince. Na průběh mají vliv kulturní a společenské podmínky. V současnosti dochází k prodloužení období závislosti na rodině. Také vrstevnické vztahy jsou pevnější, a to zejména v oblasti partnerských vztahů. V souladu s platnými právními normami je osmnáctiletá osoba označována jako plnoletá a zodpovědná za své jednání. Jde také o období hledání identity a experimentování s rolemi a hodnotami skrze zkoušení nových možností, což napomáhá upevnit jejich identitu (Vágnerová a Lisá, 2021).

1.2 PUBESCENTI A CHOVÁNÍ NA INTERNETU

Internet je vnímán jako prostředí bez zábrán, kde dospívající mohou být výřečnější a odvážnější. Přitahuje je možnost svobodného projevu, sdílení názorů, emocí a tužeb, zároveň také vnímají absenci sankcí ze strany okolí či jedinců, se kterými komunikují. Virtuální prostředí vidí jako místo pro snadné lhaní, přetvářku, změny své identity, a také místo, kde se mohou cítit v (fyzickém) bezpečí. Anonymita totiž eliminuje strach z okolí, jelikož nejsou vystaveni přímé kritice na jejich vlastní vzhled, což v dospívání hraje klíčovou roli. Na druhou stranu, pokud se dospívající bojí o svou skrytou identitu, využijí možnost anonymity a pozměnění informace o sobě. Online svět je zároveň místem pro zábavu, odreagování a experimentování s identitou, přičemž zejména pubescenti častěji lžou a vydávají se za někoho jiného. Chatovací platformy a sociální sítě jim poskytují prostor pro zkoušení různých sociálních rolí a hledání vlastní identity. Mimo to vnímají například udržování konverzace bez nějakého hlubšího smyslu jako „zkrácení volné chvíle“ (Šmahel, 2003).

1.2.1 Agresivní chování

Digitální prostor hraje významnou roli při šíření a eskalaci agresivního chování, které se u jedinců vyvíjí v závislosti na věku a sociálním prostředí. U dětí na prvním stupni základní školy bývá agrese spíše impulzivní a pramení z emoční nezralosti, rodinných problémů (rozvod, rodinná krize apod.) nebo různých poruch pozornosti či chování. Útočníci v této fázi života své útoky neplánují a jejich chování je spíše reakcí na frustraci či neschopnost zvládat emoce. Na druhém stupni základní školy jsou útoky čím dál více promyšlené a cílené. Cílem útočníka je získat dominanci ve vrstevnické skupině nebo sociální status. Obecně se může jednat o jedince, kteří vyrůstají v prostředí bez dostatečné emocionální podpory nebo jsou to naopak jedinci, kteří si tím kompenzují své vlastní neúspěchy. Jedinci na střední škole často disponují vyšší mírou sociální inteligence, což jim umožňuje efektivně skrývat své chování, které se stává komplexnějším a může být součástí sociálních strategií, včetně manipulace a psychického nátlaku (Martínek, 2015). Své oběti si vybírají zcela náhodně a často si vůbec neuvědomují, jaký může mít jejich chování dopad na někoho jiného (Kožíšek, 2016).

Agresivní chování se může na internetu objevit ve formě tzv. flamingu, kde jde o hádky ve virtuálním prostoru (podrobněji viz 2.1.1). Toto chování může zhoršit pocit frustrace, která může dále souviset s problémy s připojením k síti (Šmahel, 2003).

1.2.2 Role rodičů

Důležitou roli hrají rodiče, jelikož ovlivňují přístup dětí k užívání internetu. Snaha ovlivnit používání internetu je známá jako tzv. rodičovská mediaci, která je dále členěna na aktivní mediaci, restriktivní mediaci a tzv. technický monitoring neboli kontrolu. Aktivní mediaci zahrnuje rozhovory, kdy rodiče dítěti vysvětlují, co je na internetu to špatné a co dobré. Tento typ mediaci je považován za nejúčinnější, protože rozvíjí digitální dovednosti, zlepšuje porozumění internetu a pomáhá dítěti lépe reagovat na potencionální rizika. Restriktivní mediaci omezuje děti ve sbírání zkušeností, což může vést k nižší úrovni digitálních dovedností. Technický monitoring, známý jako tzv. rodičovská kontrola, používá speciální software, který má za úkol sbírat informace o aktivitě dítěte (Smahel et al., 2020).

Internet je pro pubescenty ideálním místem k naplnění snahy oddělit se od rodičů. Přitažlivost internetu lze odůvodnit pocitem bezpečí při poznávání nových lidí z pohodlí domova (Šmahel, 2003).

1.2.3 Negativní vlivy sociálních sítí

Osoby na sociálních sítích (viz 2.4) mohou výrazně ovlivňovat vnímání těla, a to zejména u dospívajících. Jsou spojovány s tlakem módních trendů a porovnáváním se s vrstevníky, což zvyšuje riziko rozvoje poruch příjmu potravy. Negativní vliv mohou mít na sebepojetí a zdravé stravovací návyky, a proto je prevence a edukace v této oblasti klíčová (Klepáčková, 2022).

Mezi další rizikové jevy patří nadměrné užívání sociálních sítí. Aplikace se často aktualizují a vylepšují prostřednictvím nových funkcí. To přispívá k dlouhodobému a intenzivnímu užívání, což může vést až k závislostnímu chování, jinak nazývanému netolismus (Kubala, 2019). Ten nese svá rizika, která mohou být fyzická i psychická. Existuje možnost vzniku obezity, srdečních onemocnění a bolesti páteře, což je spojováno s dlouhodobým sezením a menším až nulovým pohybem, dále poruchy zraku kvůli dlouhodobému sledování obrazovky. Mezi psychická rizika patří úzkost, deprese, zhoršení mezilidských vztahů či sociální izolace (Kopecký, c2008-2024b). I přestože se tématu digitální závislosti tato práce přímo nevěnuje, projekt E-bezpečí ji považuje za rizikový jev, proto zde byl uveden jen krátký úvod do problematiky. Veškerá další rizika budou uvedena v následující kapitole.

2 BEZPEČNOST V DIGITÁLNÍM SVĚTĚ

V digitálním světě, kde se internet stal nedílnou součástí našeho každodenního života je tematika bezpečnosti stále důležitější. S rostoucí mírou užívání internetu zároveň roste také pravděpodobnost setkání s rizikem. Proto zde budou definovány ta online rizika, se kterými se lze potkat.

Tomuto tématu se věnuje projekt E-bezpečí, zaměřený na prevenci, výzkum a šíření povědomí v oblasti rizikového chování na internetu. Je realizován Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého a dalšími organizacemi, včetně ministerstev a Policie České republiky (dále jen ČR). Soustředí se na práci se žáky, učiteli, rodiči i odborníky, pořádá přednášky, provozuje online poradnu a propojuje modelové situace se skutečnými případy. Za svou práci získal mnoho ocenění a za dobu své existence pomohl tisícům obětí kyberkriminality (Informace o projektu – E - bezpečí, c2008-2024). Typologie rizik pro tuto práci byla vybrána na základě tohoto projektu. Ten považuje za nejzávažnější tato rizika:

- kyberšikana,
- kybergrooming,
- stalking a kyberstalking,
- rizikové využívání sociálních sítí,
- dezinformace (hoax, spam, fake news).

Za další rizikové jevy autoři projektu považují:

- trolling a webcam trolling,
- fenomén youtubering,
- útoky na elektronické bankovníctví (phishing),
- online závislost (netolismus, nomofobie) (Informace o projektu - E-bezpečí, c2008-2024).

2.1 Kyberšikana

Dle Kožíška a Píseckého (2016) je kyberšikana cílené a opakované chování člověka, které má za úkol narušit psychickou pohodu prostřednictvím moderních technologií. V porovnání s klasickou šikanou, nelze útok snadno předpovědět. Útočník se totiž může skrývat pod

fiktivní identitou, kvůli které se chová méně opatrně a na rozdíl od reálného světa nevidí dopad, který to může na obětech zanechat. Často se může jednat o člověka, který v životě trpěl méněcenností, odlišoval se od ostatních nebo byl nepochopený.

Dle Priceové a Dalgleshe (2010, s. 51) je kyberšikana „kolektivní označení formy šikany, která využívá elektronické prostředky, jako je internet a mobilní telefon, které slouží k agresivnímu a záměrnému poškození uživatele těchto prostředků. Stejně jako „tradiční“ šikana, kyberšikana obvykle zahrnuje opakované chování a nerovnováhu sil mezi útočníkem a obětí.“

Od online obtěžování se kyberšikana liší svou opakovaností, dlouhodobostí a cílem ublížit oběti. Může být také nezáměrná, a to například formou nevhodného vtipu, který se následně vymkne kontrole (Co je kyberšikana?, c2008-2024). Nelze ale říci, že by online obtěžování nebylo závažné. Prevence je důležitá i v tomto případě. Opakovanost může být způsobena i diváky (tzv. přihlížejícími), kteří reagují na komentář či reagují „to se mi líbí,“ čímž prohlubují agresi. Publikování jediné fotografie či videa může mít dlouhodobé následky, protože přihlížející se k tomu neustále vracejí a obsah si přeposílají (Černá et al., 2013).

2.1.1 Projevy kyberšikany

Kyberšikana se projevuje různými způsoby, mezi které dle Policie ČR patří:

- zasílání zpráv obsahujících urážky či výhrůžky, šíření pomluv, a to prostřednictvím SMS, e-mailu či chatovacích aplikací (Messenger, Instagram, Snapchat a další),
- pořizování, upravování a následné zveřejňování fotografií, zvukových či video záznamů (může jít například o nahrávání předem naplánovaného útoku),
- tvorba blogu nebo webových stránek, které se zaměřují na urážení, zesměšňování či pomlouvání konkrétní osoby nebo skupiny osob,
- krádež identity (např. facebookového nebo instagramového účtu)
- provokativní chování, případně spamování v diskusních fórech nebo chatovacích místnostech,
- odhalování soukromých informací,
- vydírání prostřednictvím mobilního telefonu, anebo internetu,
- obtěžování formou opakovaných telefonátů a zpráv (Burýšková, 2009).

Za další formu lze považovat také flaming. Tento termín označuje velmi intenzivní hádku ve virtuálním prostředí, často na diskusních fórech nebo chatech. Jsou doprovázeny vzájemnými urážkami, nadávkami, emotivní výměnou názorů či vyhrožováním. Aby se dalo hovořit o kyberšikaně, musí mít útočník záměr cíleně poškodit oběť (Černá, 2013). Dlouhodobost hádek je zapříčiněná anonymitou útočníka. Specifickou formou provokace je tzv. flamebait, kdy je hádku záměrně vyvolána provokujícím příspěvkem (Co je flaming, 2008).

Dále sem lze zařadit tzv. happy slapping, jehož podstatou je fyzické napadnutí oběti, které je natočeno na kameru a následně sdíleno na internetu (Happy slapping, 2008). Existuje mnoho případů, při kterých takový druh ponížení na internetu měl na oběť velmi silný dopad a skončilo to sebevraždou (Černá, 2013).

2.1.2 Anonymita

Útočník svou identitu může schovat prostřednictvím přezdívek, neznámé e-mailové adresy nebo anonymního telefonního čísla. Vytvořit novou identitu je velmi jednoduché, což oběti ztěžuje zjistit, jaká osoba se za obrazovkou skrývá. To vyvolá pocit nejistoty, což může být velmi stresující. Kvůli útočnickově pocitu ochrany může útok eskalovat (Martínek, 2015). Díky své anonymitě mohou agresori komunikovat bez ohledu na své fyzické či psychické nedostatky, naopak využijí svých technických znalostí (Kožíšek, 2024). Mezi útočníkem a obětí vzniká tzv. mocenská nerovnováha. I přes zablokování útočníka nebo opuštění stránky neexistuje úplná jistota, že si útočník oběť opět nenajde nebo si nezaloží účet nový. Neznalost identity útočníka omezuje oběti možnost bránit se (Černá et al., 2013).

2.1.3 Krádež identity

Jde o získání moci nad virtuální identitou uživatele útočníkem, který získá přihlašovací údaje k e-mailu, účtu oběti na sociálních sítích, v počítačové hře apod. Pokud se mu je nepodaří získat, postačí mu pouze profilová fotka, jméno a všechny další uvedené informace a účet si založí zcela nový. Cizí identitu využije zejména k poškození oběti, kdy přidává nevhodné statusy či komentáře například na sociálních sítích. Dále má za cíl ukrást citlivá data a následně oběť vydírat (Kohout, 2017a). Pokud útočník svůj cíl splní nebo mu hrozí odhalení, tak si vytvoří identitu novou (Kožíšek, 2016).

2.1.4 Šíření citlivých dat

V dětských kolektivech může docházet k pořizování fotografií nebo dokonce k tzv. fotomontážím, které jsou následně šířeny dál. Jedinec může být zachycen v choullostivých situacích jako převlékání na tělocvik ve škole nebo při návštěvě toalety. Při šíření videí si útočník video či zvuk může poupravit, následně vyhrožuje oběti, že danou věc nezveřejní pod nějakou podmínkou. Může se jednat o kredity do hry nebo také, že se nedopustí žádného násilí na oběti. Útočníkem nemusí být jen někdo cizí, může se jednat o blízkou osobu, která za zády sdílela osobní a citlivé informace (Kožíšek, 2024). Důležité je také zmínit, že do podobných situací se nedostávají jen žáci, ale i pedagogové ve škole (Kohout, 2017b).

2.2 Kybergrooming

Dle Kožíška a Píseckého (2016, s. 72) je kybergrooming „takové chování uživatelů internetu, jehož cílem je pomocí internetových komunikačních prostředků a jiných technologií vyvolat v dospělém/dítěti pocit důvěry a prostřednictvím falešné identity ho zneužít nebo vylákat na schůzku.“

Definice E-bezpečí říká, že kybergrooming je druh psychické manipulace, při které probíhá komunikace mezi dítětem od věku 11 do 17 let a dospělým uživatelem. Ten je často pod falešnou identitou a vydává se za jejich vrstevníka. Ve většině případů byl u útočníka diagnostikován patologický zájem o děti, také asociální porucha, sexuální agrese apod. Útočník se snaží oběť přimět ke schůzce v reálném světě, kde může dojít sexuálnímu zneužití, zneužití k dětské pornografii, prostituci, fyzickému mučení, či dokonce k terorismu. Ke kybergroomingu v posledních letech dochází zejména na platformách jako je Snapchat, Skype, TikTok, Instagram, Discord a Roblox. Důležité je ovšem zmínit, že místa setkání sama o sobě nebezpečná nejsou, nebezpeční jsou uživatelé, kteří je zneužívají (Kopecký, c2007-2024).

V České republice je tento čin trestán. Dle Zákona č. 40/2009 Sb., Trestní zákoník je ten, kdo „navrhne setkání dítěti mladšímu patnácti let v úmyslu spáchat trestný čin podle § 187 odst. 1, § 192, 193, § 202 odst. 3 nebo jiný sexuálně motivovaný trestný čin, bude potrestán odnětím svobody až na dvě léta“ (Česko, c2010-2014, § 193b). Viz sexting, který je uveden níže.

Existuje mnoho manipulativních technik, které útočníci využívají (Kopecký, c2007-2024). Tyto pojmy budou rozvedeny v následujících podkapitolách.

2.2.1 Mirroring

Při této technice dochází k nápodobě chování oběti tak, aby došlo k prolomení zábran a útočník se choval podobně jako jeho oběť. Pokud oběť zmíní pocity osamělosti nebo osobní problémy, útočník často reaguje tvrzením, že oběti rozumí, protože se nachází v podobné situaci. Nabízí tak oběti možnost svěřit se, čímž vytváří iluzi blízkého vztahu. Kromě toho může předstírat podobné zájmy, názory a další, aby v oběti vyvolal větší pocit propojení (Kopecký, 2010).

2.2.2 Phishing

V souvislosti s kybergroomingem chápán jako metoda k získávání osobních a citlivých údajů k usnadnění další manipulace a zneužití oběti (Kopecký, c2007-2024). Představuje druh kybernetického útoku, u kterého útočník využívá techniky sociálního inženýrství (tzn. manipulace a klamání) k získání citlivých údajů oběti nebo k instalaci škodlivého softwaru na zařízení oběti. Tento útok se nejčastěji uskutečňuje skrze falešný e-mail, ve kterém se nachází žádost o platební údaje nebo o přihlašovací informace k internetovému bankovníctví. Phishing se ale může objevit také na sociálních sítích a chatovacích aplikacích (Phishing, c1992-2024).

Dle Kožíška a Píseckého (2016) jde o podvodnou techniku, při které se útočník snaží získat soukromé údaje, jako jsou hesla, kreditní karty a jiné. Nejčastěji užívá identitu od banky, sociální sítě, Police ČR či jiné služby s cílem zmanipulovat oběť, aby zadala své soukromé údaje na stránce, která vypadá jako pravá, ale ve skutečnosti je falešná. Pokud by útočník při svém pokusu selhal, při příštím útoku se pokusí zdokonalit, aby uspěl.

Phishing lze rozpoznat díky několika znakům. Mezi ně patří chyby v gramatice, nabídka velmi výhodné nabídky, například dědictví, zboží zadarmo, výhra v loterii nebo čekání balíku na poště. Dalším znakem může být zvláštní adresa odesílatele e-mailu. Opět se může jednat o překlep, ale ne vždy si ho lze na první pohled všimnout. Zprávy bývají často naléhavé, kdy příjemce zprávy nemá dostatek prostoru na rozmyšlenou. Posledním znakem je snaha získat citlivé údaje, což žádné instituce nikdy nezjišťují skrze e-mail nebo zprávy (Kožíšek, 2024).

Tzv. pharming je pokročilejší varianta phishingu, kdy útočník změní správnou adresu na tu svou. Osoba je přesměrována na falešný web a nevědomky se stává obětí podvodu. Pro vysvětlení se může jednat například o komunikaci s bankou nebo jinou institucí (Král, 2015).

Při phishingu může dojít k nechtěnému stažení nějakého druhu malwaru, což je jakýkoliv software, který má za cílem narušit standardní činnost systému počítače, získat data od oběti nebo dokonce získat přístup k systému počítače (Kolouch, 2016). Druhy malwaru se dále dělí na:

Adware

Neustálé a obtěžující vyskakování oken reklamy nebo webových stránek na místech, kde by se neměla nacházet, anebo umístěných tak, že zakrývají velkou část obrazovky. Může zpomalovat prohlížeč, změnit domovskou stránku vyhledávače a jiné (Adware, c1992 – 2024).

Spyware

Funguje na bázi tajného získávání informací o oběti a následném posílání těchto dat do datové schránky k útočníkovi. Útočník data dále prodává nebo je využije k dalším kybernetickým útokům (Spyware, c1992-2024). Na rozdíl od adware se nainstaluje do zařízení bez vědomí a souhlasu oběti, je také mnohem nebezpečnější a škodlivější než adware (Adware, c1992 – 2024). S největší pravděpodobností se s ním lze setkat při stahování a instalaci programů nebo her z neověřených zdrojů (Kožíšek, 2024).

Vir

Škodlivý program, který se šíří sám a bez vědomí oběti tím, že se kopíruje do dalších programů nebo dokumentů s cílem nakazit celý systém, převzít kontrolu nad systémem počítače a ukrást soukromá data oběti (Co je počítačový virus + druhy virů, c1992-2024). Projevovat se může pouštěním hudby, změnou či ničením dat až po destrukci celého systému (Kolouch, 2016). Viry se postupně začaly navrhovat tak, aby působily nenápadně a mohly popřípadě do napadnutého zařízení stahovat další škodlivé programy (Král, 2015).

Červ

Na rozdíl od viru, červ nepotřebuje žádného hostitele (spustitelný soubor) a je šířen sám pomocí rozesílání své kopie dalším obětem pomocí internetu, čímž se šíří velmi rychle, což může vést až k přetížení sítě (Kolouch, 2016).

Trojský kůň

Počítačové programy, které se stejně jako viry mohou nacházet skryté v jiném souboru. Samotný problém se neprojevuje hned a na rozdíl od viru se není schopen šířit sám bez zásahu oběti. Jakmile se trojský kůň aktivuje, může dojít k mazání, blokování, změně dat nebo

narušení systému počítače nebo internetové sítě (Kolouch, 2016). Také slouží k otevření tzv. zadních vrátek (tzv. backdoor), převzetí kontroly nad zařízením, získání dat oběti a následné odeslání útočníkovi (Trojský kůň, c1992-2024).

Keylogger

Druh škodlivého softwaru, který sleduje a zároveň zaznamenává vše, co oběť píše na své klávesnici. Záznam stisků je následně odeslán útočníkovi na server. Útočník má tak možnost získat přihlašovací údaje (uživatelská jména a hesla), čímž získá přístup do chráněných systémů oběti. Může se například jednat o sociální sítě, bankovní účty a další (Definition of Keyloggers, c2024).

Ransomware

Škodlivý program s cílem zabránit nebo omezit přístup k počítači, který nakazil. Útočník po oběti požaduje zaplacení výkupného za to, že mu opět zpřístupní jeho počítač (Kožíšek a Písecký, 2016). Nedoporučuje se ale výkupné platit, jelikož není zaručeno, že přístup k počítači bude opět zpřístupněn. Existuje totiž mnoho aplikací, které dokáží zašifrované soubory obnovit (Ransomware, c2018).

Scareware

Falešný antivirový program, který si uživatel stáhne na základě nabídky jako nezbytné ochrany jeho zařízení. Po instalaci programu funguje zkušební verze programu, která spustí falešnou kontrolu počítače. Ta detekuje až stovky infikovaných souborů, které jsou ale ve skutečnosti v pořádku. Pro jejich odstranění je uživatel pobídnut ke koupi plné verze, díky čemuž je zmanipulován k platbě za program, který žádnou reálnou ochranu neposkytuje (Král, 2015).

2.2.3 Profiling

Útočník si vytvoří profil dítěte tak, aby byl co nejvíce podobný skutečným dětem. Nejprve si udělá analýzu zájmů, koníčků a osobních údajů dítěte, aby si vytvořil důvěryhodnou identitu. Následně začne oslovovat své oběti, kterých bývá současně několik, což mu umožňuje efektivně rozšiřovat svůj dosah a manipulovat s větším množstvím obětí (Kopecký, c2007-2024).

2.2.4 Luring

Luring neboli vábení a uplácení oběti je spojeno s navázáním vztahu s obětí pomocí různých dárků a úplatků. Konkrétně se může jednat o peníze, kredit do mobilního telefonu, koupě počítačové hry, nového mobilního telefonu, oblečení a další. Přes tyto úplatky útočník snadno získá osobní údaje, jako je telefonní číslo nebo adresa oběti, kam právě zašle dárek (Szotkowski et al., 2013). Existují případy, kdy se oběti kvůli nabídkám k útočníkovi opakovaně vracely, čímž podlehly dalšímu zneužívání. V takových situacích lze hovořit o formě dětské prostituce (Kopecký, 2010).

2.2.5 Sexting

Sexting je definován jako posílání fotografií, či videí a textových zpráv se sexuálním obsahem. Jeho důsledky mohou být až fatální, proto je považován za jedno z nejrizikovějších. Materiály nahrané na internet je prakticky nemožné smazat, proto se kdykoliv mohou objevit znovu (Kožišek a Písecký, 2016). Může jít také o vzájemnou výměnu nahých nebo polonahých fotografií, videí, či zpráv přes mobilní telefony a sociální sítě. Samo o sobě to rizikové chování být nemusí. Může jít pouze o součást sexuálního vývoje dospívajících. Pokud to ale přejde do stádia vydírání, či dokonce rozeslání materiálu, může jít o velký problém a mít negativní dopad na psychický stav oběti (Hollá, 2021).

Sexting je považován za trestný v případě, že osoba „přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, bude potrestán odnětím svobody až na dva roky“ (Česko, c2010-2014, § 192), přičemž bude platit stejný trest pro toho, kdo vůbec k takovému materiálu získá přístup. Pokud jedinec „vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, anebo kdo kořistí z takového pornografického díla, bude potrestán odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci“ (Česko, c2010-2014, § 192).

2.2.6 Izolace oběti

Útočník se díky své anonymitě stane blízkým přítelem oběti a manipuluje ji citovým nátlakem, aby žádnou informací neříkala rodičům nebo jiným blízkým. Postupně to přejde do závislosti na útočníkovi. Při snaze komunikaci přerušit, útočník začne s vydíráním, že

vyzradí tajemství oběti. Oběť tedy nadále pokračuje v komunikaci a je manipulována k osobní schůzce (Szotkowski et al., 2013). Pachatel se snaží dítě od rodičů izolovat nejen fyzicky, ale i psychicky, kdy dojde ke zhoršení komunikace s rodiči nebo tráví více času na počítači. Typickými frázemi jako „neříkej to rodičům, nepochopili by to“ nebo „pokud jim to prozradíš, budeš mít problémy“ udržuje dítě v izolaci, čímž postupně narušuje jeho důvěru v rodinu a blízké okolí (Kopecký, c2007-2024).

2.2.7 Lákání skrze fotografii opačného pohlaví

Aby se útočník skryl, použije falešný profil. Podle své oběti si na profilu změnil své pohlaví. V průběhu komunikace útočník vyzve svou oběť, zda si nechce vyměnit své intimní fotky. Následně je sám pošle, ale jedná se samozřejmě o falešnou fotografii. Dítě na to pak zareaguje stejně a pošle svou intimní fotku, čímž útočník získá prostředek k vydírání (Kopecký et al., 2015).

2.2.8 Webcam trolling

Útočník se snaží získat intimní fotografie či video od své oběti. Využívá k tomu speciální program simulující webkameru, aby oběť oklamal falešnými videi reálných lidí z videochatů. V důvěrné atmosféře oběť ukáže intimní záběry, které si útočník nahraje a později je použije k vydírání (Szotkowski et al., 2013).

2.3 Stalking a kyberstalking

Dle Policie ČR jde o „opakované stupňované obtěžování, které může mít různou podobu a intenzitu“ (Hašlová, 2020). Může mít různé formy a různou intenzitu. Pokud je při stalkingu použita jakákoliv informační a komunikační technologie, lze hovořit o kyberstalkingu (Co je to stalking a cyberstalking, 2008). Mezi typické projevy stalkingu patří:

- opakovaný pokus o kontakt s obětí (dopisy, telefonáty, SMS zprávy, zasílání dárků ad.),
- (ne)přímé výhružky, které mohou v oběti vyvolat strach a obavy,
- vyhledávání blízkosti oběti (postávání v blízkosti bydliště, zaměstnání, sledování),
- ničení osobního majetku oběti,

- zneužívání osobních údajů oběti např. zveřejnění telefonního čísla, adresy ad. na internetu s falešnými informacemi (např. prodej bytu, nabídka sexuálních služeb) (Frýdecká, 2009).

Stalking je vysoce nebezpečné chování, které by se v žádném případě nemělo podceňovat. I nejprve nevinná „hra“ může mít tragické následky. Pro odborníky je často složité odhalit rozdíl mezi nevinným pokusem o kontakt a skutečným nebezpečným pronásledováním (Kožíšek, 2016).

Obsah stalkingových zpráv nemusí být vždy zastrašující, ale může nabýt také přátelské, příjemné a veselé atmosféry. Útočnickovým cílem je ale vyvolat strach v oběti. Mezi konkrétní příklady zpráv Kožíšek (2024) uvádí tyto: „Moc se mi líbíš, pořád se dívám na tvoje fotky,“, „Ty mi vážně nebudeš odepisovat?“ „Jestli mi neodepíšeš, tak si ublížím!“ a mnohé další.

Tento pojem je také chráněn legislativou, a to konkrétně zákonem č. 40/2009 Sb., trestní zákoník. Tam je nebezpečné pronásledování definováno jako dlouhodobé obtěžující chování, které může zahrnovat vyhrožování újmou, sledování, opakované kontaktování prostřednictvím různých prostředků, omezení běžného způsobu života či zneužití osobních údajů. To může být trestáno odnětím svobody až na jeden rok nebo zákazem činnosti. Pokud ovšem je tento trestný čin spáchán vůči dítěti, těhotné ženě nebo dvěma a více osobám či dokonce se zbraní, může odnětí svobody trvat od šesti měsíců do tří let (Česko, 2009).

Nejčastěji se vyskytuje u nezadaných nebo čerstvě nezadaných lidí, ale setkat se tímto problémem může kdokoli, nezáleží na společenském postavení, genderu ani věku. Důsledky (kyber)stalkingu se často projevují psychickými a fyzickými obtížemi a dopadem na chování oběti, jako je nervozita, úzkost, deprese, panické ataky, poruchy spánku, vztek a agrese. Obtěžování navíc vede k poklesu sebeúcty a sebehodnocení. Psychická zátěž se může odrazit na fyzickém zdraví jako je častá bolest hlavy, žaludeční nevolnosti, zvracení či kožní vyrážky vyvolané psychickým tlakem. Oběť také může změnit své chování vůči kyberprostoru na vyhýbavé chování a snahu minimalizovat jakýkoliv kontakt se svým okolím. Může dojít k rizikovému chování trávení volného času, například nadměrná konzumace alkoholu, přejídání či užívání drog (Martinek, c2025).

2.4 Rizikové využívání sociálních sítí

Nejprve je třeba definovat pojem sociální síť. Tu lze definovat jako virtuální prostor, který umožňuje registrovaným uživatelům vzájemně komunikovat, sdílet informace, fotografie nebo videa (Sociální sítě, c2024). Slouží k vyjadřování názoru na různá témata, komentování příspěvků a diskutování v různých skupinách a fórech (Sociální sítě, b. r.). Ve světě existuje nespočet sociálních sítí a větší část z nich slouží jen k sebeprezentaci nebo zábavě, ale také k profesnímu, seznamovacímu účelu nebo třeba jen určité skupině lidí (např. cyklisté, lidé vlastnící psa, sběratelé apod.) (Kožíšek, 2024).

Konkrétně lze mezi sítěmi jmenovat například tyto:

- **Facebook** – celosvětově nejpoužívanější síť umožňující sdílet příspěvky, fotografie, videa, komentáře, vytvářet události, skupiny, a komunikovat skrze zprávy.
- **Instagram** – vizuálně orientovaná síť zaměřená na sdílení fotografií, videí a tzv. „stories“, která umožňují sdílet obsah na 24 hodin, využívá se také k marketingu.
- **YouTube** – největší platforma ke sdílení videí, která poskytuje prostor k nahrávání, sledování a interakci s obsahem (komentář a hodnocení videa skrze palec nahoru nebo dolů).
- **X** (dříve Twitter) – funguje na základě krátkých textových příspěvků, které také mohou obsahovat video či fotografii, je využíván pro sdílení aktuálních zpráv, diskusí nebo názorů.
- **TikTok** – je určen ke sdílení krátkých videí, která mohou být doplněna také hudebním podkresem, popularitu má zejména u mladších uživatelů.
- **Snapchat** – slouží pro sdílení dočasných fotek a videí, které se po zobrazení smažou, lze použít různé filtry (Redakce Sitevhrsti.cz, 2020).
- **Discord** – je určen k hlasové a textové komunikaci zejména pro hráče her, ale má široké využití i mimo tuto uživatelskou skupinu.
- **Twitch** – je platforma pro živé vysílání především zaměřená na herní obsah, při vysílání mohou diváci komunikovat mezi sebou a také s vysílajícím (Šimek, 2022).

Na sociálních sítích lze narazit na osoby, které se lidem snaží předat něco užitečného, vzdělávat ostatní nebo s nimi komunikovat a udržovat spojení se svými stávajícími kamarády nebo si najít kamarády nové (Slussareff, 2022). Kromě toho ale přináší svá rizika,

kteřá jsou často spojena s neobezřetností uživatelů, jelikož nechtou podmínky spojené s jejich užíváním sociálních sítí a neuvědomují si, že jejich sdílené osobní údaje jsou snadno dohledatelné dalšími uživateli (Sociální sítě, c2018).

Digitální platformy mají zásadní vliv na tvorbu dopaminu, známého jako „hormon štěstí“, který lidem přináší pocit uspokojení, zmírňuje stres a často funguje jako forma odměny. Tento mechanismus může vést až do bodu závislosti, čímž se oslabuje přírodní zdroj získávání dopaminu. Mezi zdroje patří například sport, pobyt v přírodě, či kreativní aktivity. Z dlouhodobého hlediska mohou mít sociální sítě dopad na psychické zdraví, častou únavu, úzkosti nebo deprese, jelikož často vytvářejí iluzorní obraz dokonalosti, což může vést k negativním pocitům a srovnávání s ostatními. Proto je vyváženost mezi online a off-line klíčová (Petráková, c1994–2024).

Na sociálních sítích se mohou uživatelé setkat s krádeží účtu, přičemž útok je nejčastěji cílen na veřejně známé osoby. To nemusí znamenat krádež účtu, ale jeho zneužití k sledování jiných účtů. Zneužití účtu lze poznat podle sledování falešných nebo nevhodných účtů (Kubala, 2019). Ukradené údaje mohou být dále prodány dalším zločincům, kteří s nimi dále obchodují (5 způsobů krádeže hesel a jak se bránit, 2022).

2.5 Dezinformace

V dnešní době mohou být lidé sami svědky nárůstu informací, které se šíří rychlostí jednoho kliknutí. Tím se také zvyšuje riziko toho, že ne všechny informace šířené po internetu budou zcela pravdivé. V úvodu bude definován pojem dezinformace, jelikož je zastřešující pro pojmy další.

Dle Evropské komise (2022, s. 24) jsou dezinformace „prokazatelně nepravdivé nebo zavádějící informace, které jsou vytvářeny, předkládány a šířeny za účelem ekonomického prospěchu nebo úmyslného klamání veřejnosti. Mohou způsobit veřejnou újmu.“

2.5.1 Spam

Spam je nevyžádaný typ komunikace skrz e-mail, SMS, sociální sítě a další. Obvykle obsahuje reklamní sdělení a je často rozesílán bez souhlasu příjemce (Spam, c1992-2024). Může obsahovat jakoukoliv formu malware, pornografické, edukační, politické, náboženské, finanční a další informace. Podvodný nebo kriminální obsah se označuje jako scam, jehož cílem je získat důvěru a donutit ho vykonat něco, o co podvodník žádá. Například rozkliknutí odkazu v příloze zprávy (viz Phishing) (Kolouch, 2016).

☐	LD	LDt6vm@seznam.cz	☆ gabca.klagova Zaregistrujte se za pouhých 30 sekund. 100% ZDARMA – Je to ...	Včera 13:06
☐	XY	xYWrF@seznam.cz	☆ gabca.klagova 3 měsíce ZDARMA – Zaregistrujte se nyní za poplatek Poté 10,99 E...	Včera 8:25
☐	HG	hgBHpXOHFcVmo@sezna...	☆ gabca.klagova Zaregistrujte se za pouhých 30 sekund. 100% ZDARMA – Je to m...	Včera 5:14
☐	NJ	NjanlfgF@seznam.cz	☆ gabca.klagova Zaregistrujte se za pouhých 30 sekund. 100% ZDARMA – Je to ...	22. 3. 2025
☐	HB	HBdPnVHvutSX@seznam.cz	☆ gabca.klagova Bonus kasina 50 % – Hrajte online kasino se skutečnými penězi S...	22. 3. 2025
☐	TV	tVYpcwo@seznam.cz	☆ gabca.klagova Gratuluji – Akademie výcviku důstojníků (OTA) hvězda teď tady ob...	22. 3. 2025
☐	YL	Ylnzk1XCMRT4Ut@sezna...	☆ gabca.klagova 🏆 🏆 ZAHRAJTE SI AŽ 5000+ KASINOVÝCH HER S KRYPTOMĚNOU: BITC...	22. 3. 2025
☐	9L	9l64CbPO9Gn2N@sezna...	☆ gabca.klagova Bonus kasina 50 % – Hrajte online kasino se skutečnými penězi S...	22. 3. 2025
☐	F0	F0gbZMQ15k0O@seznam....	☆ Annual Leave Report For 2025 – Obsah pro dospělé Skutečné obrázky krásce ve ...	22. 3. 2025
☐	OV	OvutBviF7@seznam.cz	☆ gabca.klagova 🏆 🏆 ZAHRAJTE SI AŽ 5000+ KASINOVÝCH HER S KRYPTOMĚNOU: BITC...	22. 3. 2025
☐	HV	HV7S7T9pRc@seznam.cz	☆ Annual Leave Report For 2025 – Obsah pro dospělé Skutečné obrázky krásce ve ...	21. 3. 2025

Obrázek 1 Ukázka spamu

(zdroj: vlastní)

2.5.2 Hoax

Jedna z forem spamu používaná k označení řetězových zpráv, které bývají masově šířeny s výzvami typu: „pokud to nepřešleš dál, stane se...“ Zprávy tohoto typu často obsahují nepravdivé informace, které mohou vyvolat paniku, například varování před útoky a nebezpečím, petice, řetězové dopisy štěstí, prohlášení slavných osobností a další (Kolouch, 2016). Dále varování před nejničivějším počítačovým virem, migrační vlna, válka, nebezpečí skryté ve vašem počítači a další (HOAX, 2016). Lze ho chápat jako zprávu poplašnou (Mareš, 2022).

2.5.3 Fake news

Termín fake news (neboli falešné zprávy) označuje nepravdivé zprávy a média. Důležité je ovšem zdůraznit, že se nejedná o satirická, či humoristická média, jejichž obsah je zpravidla označen jako fikce (Kopecký, 2022a). Lze to tedy brát jako zprávu falešnou (Mareš, 2022).

2.6 Fenomén youtubering

Platforma YouTube patří mezi největší sociální sítě zaměřené na videoobsah. Umožňuje uživatelům příspěvky komentovat, hodnotit (pozitivně nebo negativně) a také sdílet. Mezi nejčastější typy obsahu patří hudební videa, vlogy, vzdělávací materiály, tutoriály nebo třeba záznamy z hraní her (YOUTUBE, c2024).

Obavy týkající se platformy YouTube jsou často podobné těm, které se týkají ostatních sociálních sítí jako jsou Facebook, Instagram nebo Snapchat. Může zahrnovat nevhodné či problematické projevy jako je šikana (respektive kyberšikana), pornografii,

projevy nenávisti, sebepoškozování, či sebevražda. Mohou také čelit výhrůzkám násilí či zneužívání. Výzvy jako je „Try not to laugh“ neboli „Zkus se nezasmát“ často zesměšňují druhé, což může děti vést k nápodobě a nesprávnému vnímání hranic humoru a respektu k ostatním (Preece, 2017). Tyto výzvy se mohou vyskytnout také na dalších sociálních sítích. Aktuálně např. probíhá nebezpečná výzva v některých evropských zemích včetně ČR na sociální síti TikTok. Výzva spočívá v motivaci dětí k předávkování paracetamolem, což může vést k závažnému poškození až selhání jater nebo smrti (Zdravotnická záchranná služba Olomouckého kraje p.o., 2025).

Osoby, které publikují na těchto platformách, jsou nazývány Youtuber, influencer, nebo třeba streamer. Tyto pojmy se od sebe mohou trochu lišit, proto je třeba je zde definovat:

- **Influencer** – osoba, která prostřednictvím svých názorů, postojů a také sdíleného obsahu ovlivňuje online veřejnost. Často z koníčku přechází k profesi. Kromě celebrit to mohou být také odborníci (doktor, učitel nebo pacient). Firmy je často využívají k placené propagaci produktů (Influenceři: vlivní kreativci z internetu, 2022). Influencer je zastřešujícím pojmem, jelikož se jím může stát také youtuber, streamer, tiktokér a další (Rybářová, 2020).
- **Streamer** – člověk, který skrze platformu na internetu (Twitch, YouTube, či TikTok) vysílá živě svůj obsah, který diváci sledují a současně spolu interagují a také ho mohou finančně podpořit (jednorázovým příspěvkem, nákupem předplatného či třeba koupí kusu oblečení). Tento rostoucí fenomén je klíčovou součástí online prostředí a podporuje edukaci propojením různých sociálních a geografických skupin (Streamer/ka, b. r.).
- **Youtuber** – tvůrce obsahu na platformě YouTube, kde publikuje videa a buduje svou komunitu sledujících. Ti úspěšní mohou svůj obsah zpoplatnit, vydělávat reklamou či sponzoringem, čímž výrazně ovlivňují digitální kulturu a trendy (Kdo je to Youtuber?, c2008-2024).

Dospívající tyto osoby vidí jako obvyčejné sobě rovné mladé lidi, kteří tvoří svůj obsah na internetu. Také je mohou brát jako vzor (Westenberg, 2016). Jejich chování má významný vliv na současnou online generaci. Především u dětí mladšího školního věku dochází ke snaze se setkat s těmito osobami, kupují od nich produkty (trička, mikiny, náramky atp.). Častokrát je také napodobují, také dochází k okamžité interakci, proto může docházet

k identifikaci s youtuberem. Marketingové společnosti tuto moc využívají k propagaci svých produktů (Bradáčová, 2020). Lze tedy říci, že děti a dospívající mají v tyto osoby důvěru a mohou ovlivnit některá jejich rozhodnutí a názory, např. při nákupu produktů.

2.7 Důsledky rizik

Setkání s doposud zmíněnými riziky mohou mít na jedince výrazný dopad. Z tohoto důvodu bude v této podkapitole věnována pozornost dopadům rizik v online světě na oběť. Součástí bude také typologie emocí, která je mimo jiné také použita v praktické části této práce.

Například kyberšikana může mít dopad jak emoční, fyzický, tak i dopad na chování. Jelikož je tento zážitek pro oběť velmi stresující, může to mít dopad na zdraví, kdy se jedinec může potýkat s horší koncentrací (Černá, 2013). To může vést ke zhoršení školní výkonnosti a v některých případech se také objevuje záškoláctví nebo časté absence (Gajdošová, 2011). Dále se může také setkat s bolestmi hlavy, opakovanými bolestmi břicha, nevolnostmi či s potížemi se spánkem (Sourander, 2010). Lze pozorovat rozdíl oproti klasické šikaně, která má viditelné stopy po útoku. Oběť je často po zážitku kyberšikany uzavřená a téměř přestane komunikovat se svým okolím (Kožíšek, 2016).

Goleman (2011) uvádí jako hlavní lidské emoce hněv, smutek, strach, radost, láska, překvapení, rozhořčený odpor a hanba. Dále také ke každé řadí i několik dílčích emocí. Černá et. al (2013) ale řadí mezi trvalejší emocionální dopady kyberšikany úzkost, pocit osamělosti, deprese, hněv, frustrace, a hlavně také strach, přičemž Gajdošová (2011) hovoří o duševní nestabilitě a agresivních reakcích k okolí oběti (slovní i fyzické). Lze si všimnout omezení pohybu na sociálních sítích či svém mobilním telefonu. Zejména u dívek dochází k omezení kontaktu s vrstevníky a neochotě navazovat nové vztahy.

Pro děti jakožto oběti kybergroomingu bývá těžké a bolestivé rozpoznat, že jde o zneužívání. Často pocítují lásku a na útočníka nejsou naštvané. To by mohlo zapříčinit pocit viny, že za zneužívání mohou právě oni, a právě o tento pocit útočnickovi jde. Při odhalení, že jde o zneužívání, dítě naopak pocítuje hněv nebo smutek z důvodu ztráty kamaráda (Jansen, 2011). Dále třeba u sextingu může dojít k poškození pověsti, což může mít dopad do budoucna např. při hledání povolání či vysoké školy. Také třeba k veřejné hanbě, samotné kyberšikaně i vydírání (Consequences of Sexting, c2025).

3 PREVENCE A OCHRANA V DIGITÁLNÍM SVĚTĚ

V současné době se digitální technologie staly nedílnou součástí každodenního života. Otázka prevence a ochrany v digitálním světě je proto naprosto klíčová. V této kapitole budou proto rozebrány konkrétní opatření, která uživatelům umožní předejít hrozbám, popřípadě vyřešit již vzniklé problémy na internetu. Nejprve budou zmíněna opatření, která lze vnímat jako primární a sekundární prevence. Sekundární zejména z toho důvodu, že pubescenti se již v tomto „rizikovém“ prostředí pohybují, a následně také i terciární prevence. Bude také uvedena osvěta a s ní spojené organizace, projekty nebo metodické postupy.

3.1 Desatero bezpečného chování na internetu od e-bezpečí

Prostředí internetu ukazuje plno možností využití. Mezi ně lze zařadit objevování nových věcí, učení se, hraní her, komunikaci s přáteli, ale také poznávání nových lidí. Tak jako v reálném světě, i v tom digitálním je potřeba se umět chránit. Proto bylo e-bezpečím sepsáno Desatero bezpečného chování na internetu, které uvádí základní pravidla pro pohyb na internetu, která je potřeba dodržet k zajištění bezpečí (Kopecký, c2008-2024a).

3.1.1 Ochrana osobních údajů

Veškeré informace, které se objeví na internetu mohou být kdykoliv zneužity a použity k identifikaci, sledování nebo ke krádeži identity. Je třeba mít na paměti, že existuje určitá pravděpodobnost, že se informace dostanou do rukou osobě s nečestnými úmysly. Tyto údaje tvoří tzv. digitální stopy, mezi které řadíme například celé jméno, adresu, telefonní číslo nebo rodné číslo (Kopecký, c2008-2024a). Jsou to informace, které za sebou zanechávají lidé při používání internetu, jako fotografie, telefonní číslo či detaily o každodenních aktivitách ad. Nelze je nikdy stoprocentně vymazat, proto je důležité si rozmyslet vhodnost sdílení některých informací (Kožíšek, 2024).

3.1.2 Silná a unikátní hesla

Bezpečná hesla by měla být tvořena kombinací velkých i malých písmen, čísel a speciálních znaků. Doporučuje se využívat heslo ve formě fráze složené z několika nesouvisejících slov či krátkých vět a mělo by se snadno zapamatovat, ale ne příliš jednoduše (Kopecký, c2008-2024a). Hesla se nesmí skládat z osobních údajů nebo známých informací jako je datum či

rok narození, adresa, jméno domácího mazlíčka, oblíbená kniha nebo film a jiné. Ideální délka je 15 znaků, méně znaků by bylo jednodušší prolomit (Kožíšek, 2024).

3.1.3 Dvufaktorové zabezpečení účtů

Dvufaktorové ověření představuje další úroveň ochrany účtů na internetu. Při přihlašování na účet (např. Instagram nebo TikTok) je po uživateli vyžadován kód, který mu byl zaslán na e-mail nebo mobilní telefon (Kopecký, c2008-2024a). Na modernějších zařízeních to může být otisk prstu, biometrický sken obličeje nebo potvrzení skrze další aplikaci (Kožíšek, 2024).

3.1.4 Opatrnost při internetovém seznamování

V dnešní době je seznamování na internetu zcela běžné. Je však nutné si ověřit, s kým komunikace probíhá. Při nepříjemné komunikaci je důležité ihned daného člověka zablokovat (Kožíšek, 2024). Je totiž možné, že se jedná o člověka s falešnou identitou a nebezpečnými úmysly. Je potřeba obezřetnosti a nenechat se oklamat lichotivými sliby či atraktivním vzhledem (Kopecký, c2008-2024a).

Je nutné chránit své soukromí, kontrolovat nastavení sociálních sítí a sdílet pouze nezbytné informace, jinak je velká pravděpodobnost vzniku obtěžování nebo stalkingu. Útočníkovi by mohla postačit i nevinná informace jako je jméno mazlíčka nebo datum narození k prolomení hesla. Při přidávání cizích osob do přátel je třeba dbát na opatrnost, neklikat na podezřelé odkazy nebo přílohy. Osobní setkání je nutné naplánovat na veřejném místě a informovat o tom někoho z blízkých (např. sdílením polohy). V případě nepříjemného pocitu by schůzka měla být neprodleně ukončena (Lamb-Hall, 2023).

3.1.5 Odesílání intimních fotografií a videí

I když útočníci slibují žádné šíření intimních fotografií nebo videí, je potřeba si zapamatovat, že intimní fotografie a videa se nikdy nikomu neposílají. Jakmile je tento obsah odeslán, odesílatel nad ním ztrácí kontrolu, což může vést až k vydírání a vyhrožování. Proto je nezbytné si chránit své soukromí a nikdy nepodlehnout tlaku k odeslání intimního obsahu (Kopecký, c2008-2024a).

3.1.6 Důvěra

Na internetu se nachází velké množství falešných zpráv, dezinformací a hoaxů. Proto je doporučováno si ověřovat informace na důvěryhodných zdrojích a nešířit nepravdivé

informace dál (Kopecký, c2008-2024a). Při obdržení tohoto typu zprávy, je potřeba se zamyslet, zda dává smysl. Doporučuje se vyhledat zprávu ve vyhledávači. Pokud o události píší i jiné stránky (noviny, weby a další), je pravděpodobně pravdivá, a pokud si uživatel není jistý, neměl by sdílet ani vyjadřovat souhlas bez rozmyslu (6 tipů, jak nenaletět fake news a hoaxům, b. r.). Titulky článků jsou často navrženy k upoutání pozornosti, a proto je důležité se neřítit jen titulky a přečíst si celý text, čímž lze zabránit šíření dezinformací. Při ověřování informací je důležité se zaměřit také na zdroje. Před sdílením informace je třeba se zamyslet, zda tento čin nebude považován za trestný čin (tzn. šíření poplašné zprávy, vyhrožování a další) nebo zda nemůže někomu ublížit (Kopecký, 2022b).

3.1.7 Slušné chování a respekt k druhým

Uživatelé by se měli na internetu chovat stejně slušně jako v reálném životě. To znamená, že by mělo být s ostatními zacházeno s respektem, nepsat nenávistné komentáře, neurážet a nepodílet se na šikaně. Zkrátka je důležité se chovat tak, jak by si každý přál, aby bylo zacházeno s ním. Za obrazovkou jsou totiž reální lidé a některé činy na ně mohou mít dopad. Vyjádření názoru by mělo být respektováno, pokud ale dochází k obtěžování, je vhodné situaci nahlásit a dotyčného zablokovat (Kopecký, c2008-2024a).

3.1.8 Podezřelé odkazy a přílohy

Pokud uživatel obdrží nečekaný odkaz nebo přílohu, je důležité dbát na velkou obezřetnost. Mohou v nich být totiž obsaženy škodlivé programy, které mohou poškodit zařízení nebo zneužít osobních údajů, což může mít dopad na uživatele. Před otevřením je potřeba si ověřit, zda odkaz nebo příloha pochází z důvěryhodného zdroje (Kopecký, c2008-2024a). Doporučuje se například myší najet na odkaz, ale neklikat na něj. Následně se zobrazí náhled stránky, která by se zobrazila po rozkliknutí, čímž lze předejít případnému stažení malwaru (viz 2.2.2) (Kožíšek, 2024).

3.1.9 Opatrnost při online nakupování

I přes jednoduchost a pohodlnost, je potřeba si dát pozor na nakupování z ověřených a důvěryhodných stránek se zabezpečenou platbou. Uživatelé mohou upozornit velmi nízké ceny produktů či velmi výhodné nabídky. Před nákupem by mělo být ověřeno, zda stránka využívá bezpečnostní protokol HTTPS (Kopecký, c2008-2024a). Ten přenášená data šifruje a chrání před zneužitím. Lze ho poznat podle ikony zámku vedle webové adresy (Kodůusková, 2024).

3.1.10 Žádost o pomoc

Při setkání se znepokojujícím či nepříjemným obsahem je důležité se svěřit důvěryhodnému člověku. Z pohledu dětí či dospívajících se doporučuje svěřit se rodičům nebo jinému dospělému, kterému dítě věří. Lze tak snáze nalézt řešení k problému (Kopecký, c2008-2024a).

Na tyto situace člověk není nikdy sám, existuje totiž mnoho organizací, které poskytují právě tuto pomoc a podporu. Je potřeba si uvědomit, že je v pořádku vyhledat pomoc a snažit se ochránit sebe samého. Mezi tyto organizace patří například Linka bezpečí (Linka bezpečí, c1994–2025), E-bepečí (E-Bepečí, c2008-2024) nebo třeba Bílý kruh bezpečí (Bílý kruh bezpečí, b. r.). Dále také projekt Bud' safe online, realizovaný společností Avast, který poskytuje informace, tipy i kurz pro bezpečné chování v online světě (Bud' safe online, c2025).

3.2 Antivirové programy

Král (2015) mezi základní obranu proti všem útokům (viz 2.2.2) řadí pravidelnou aktualizaci operačního systému zařízení a používání kvalitního aktualizovaného antivirového programu, jelikož se malwary neustále vyvíjí. Zároveň je potřeba mít program stažený z důvěryhodného zdroje, jinak by mohl být škodlivý. V počítači je třeba si také všimnout případných změn, které mohou signalizovat přítomnost škodlivého programu, například nárůst přenosu dat, zpomalení systému nebo zvýšená aktivita pevného disku. Mezi požadavky na kvalitní antivirový program řadí Král ochranu v reálném čase, aktualizaci a cenovou dostupnost. Ochrana v reálném čase znamená, že by antivirový program měl neustále běžet na pozadí a chránit zařízení před hrozbami. Na trhu je dostupných několik kvalitních bezplatných antivirových programů, přičemž nabízí placené verze s širším spektrem služeb, které mohou být v bezplatné verzi omezeny (např. Avast, AVG nebo ESET).

3.3 Osvěta

Ministerstvo školství, mládeže a tělovýchovy (dále jen MŠMT) vydává metodická doporučení k prevenci, např. dokument MŠMT č.j.: 21291/2010-28. Ten se zaměřuje na primární prevenci rizikového chování, součástí kterého jsou přílohy zaměřené např. na kyberšikanu a další formy kybernetické agrese, poruchy příjmu potravy, netolismus nebo třeba vandalismus, záškoláctví, návykové látky a další. Dokument obsahuje metodické

postupy pro prevenci a intervenci v těchto oblastech, včetně návodů pro práci s dětmi potýkající se s některým ze zmíněných problémů. Dále také zahrnuje již zmíněné přílohy s konkrétními nástroji, jako jsou krizové plány či důležité kontakty, na které se lze obrátit v případě týrání, zneužívání a zanedbávání dítěte ve škole, či dokonce šablony pro oznámení problému na Policii ČR nebo Orgán sociálně-právní ochrany dětí. Dokument klade důraz na dlouhodobou a systematickou prevenci, která by měla být pravidelně vyhodnocována a upravována podle potřeb konkrétní školy (MŠMT, c2013 – 2025). Školní vzdělávací program obsahuje minimální preventivní program, který je přizpůsoben specifickým potřebám a kulturním, sociální a politickým podmínkám konkrétní školy či školského zařízení. Stanovuje konkrétní dlouhodobé a krátkodobé cíle a je navržen tak, aby byl prakticky proveditelný. Jeho cílem je omezit výskyt rizikového chování a posílit schopnost žáků a studentů se chovat zodpovědně (Miovský, 2012).

Zároveň také existuje podpora školám, jako je organizace Replug me, která pořádá workshopy jak pro školy (žáky i pedagogy), tak pro rodiče. Klade důraz na šíření osvěty v oblasti závislosti v digitální oblasti se snahou mít zdravý vztah k technologiím i sobě samému. Organizace vede také výzkumy a poskytuje individuální poradenství (Replug me, [2020]). Dále také již zmíněný projekt E-bezpečí (E-Bezpečí, c2008-2024) nebo projekt DIGIDĚTI pod vedením Jana Krsňáka. Ten nabízí pro žáky či studenty, učitele i rodiče besedy s cílem zlepšit porozumění digitálnímu světu, jeho rizicích a vlivu, i jaký tento svět může být v budoucnu (Digiděti, [2018]). Lze také zmínit mezinárodní online časopis *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* s šéfredaktorem Davidem Šmahelem, vydávaný Masarykovou univerzitou. Zaměřuje se na výzkum spojený s psychosociálními aspekty používání informačních a komunikačních technologií, přičemž publikované studie pochází z různých vědních oblastí jako je psychologie, sociologie, informatika ad. (Časopis Cyberpsychology, c2025).

3.4 Pomoc při řešení vzniklého problému

I přestože preventivní opatření mohou výrazně snížit pravděpodobnost setkání s rizikem, nelze tuto možnost zcela eliminovat. Právě proto se v této podkapitole zaměří na řešení již vzniklých problémů s cílem minimalizovat škody a zabránit opakování setkání, což spadá do kategorie terciární prevence.

3.4.1 Podpora oběti

Pokud se někdo stane svědkem jakékoliv rizikové situace v online prostředí, je nezbytné zakročit a neignorovat situaci. Tento pasivní přístup může z přihlížejícího udělat spolupachatele, ať už s daným chováním souhlasí, nebo ne. Je třeba nabídnout oběti pomoc a dát najevo, že kyberšikana je nepřijatelná a musí být zastavena, konkrétně lze pomoci při nahlášení útoku apod. (Jak se chránit před kyberšikanou a jak se bránit kyberútočníkům, 2009).

Děti, které se stanou obětí šikany často váhají, komu se svěřit, jelikož po incidentu ztratí důvěru ve své okolí a mají strach ze zlámání rodičů, zhoršení situace nebo zesílení útoků. Pokud se dítě rozhodne se svěřit, obvykle volí vrstevníky nebo rodiče. V mnoha případech však nedochází ke správné ochraně a podpoře dítěte, a to zejména z důvodu nedostatečné znalosti a orientace v digitálním prostředí nebo z důvodu nejistoty efektivnosti práce (Jandová, c1994–2025). Ani uplatnění více strategií najednou nemusí vždy vést ke snížení rizika kyberšikany či jiných rizik. Otevřená komunikace mezi rodičem a dítětem může pomoci získat důvěru a odvahu se svěřit v případě potíží. Společné řešení problému může vést k lepší obraně. Na druhou stranu je důležité najít rovnováhu mezi podporou a kontrolou, protože nadměrná restrikce může vést ke ztrátě důvěry a snížení ochoty se svěřit rodiči s problémem (Černá et al., 2013).

Linka bezpečí doporučuje věnovat pozornost chování dítěte při komunikaci online, a hlavně jeho reakci na přítomnost dospělého. Doporučuje také používat filtrační a blokovací software a poskytovat edukaci o pravidlech bezpečného používání internetu (Jandová, c1994–2025). Z toho vyplývá, že Linka bezpečí se zaměřuje na kombinaci aktivní mediace a technického monitoringu, což považuje za efektivní způsob podpory.

3.4.2 Eliminace následků

Obecně je doporučováno ukončit komunikaci s danou osobou. Jakékoliv pokusy o odrazení útočníka, například vyhrožování či pomsta, by mohli intenzitu útoku zvýšit. Je kladen důraz na pasivitu a potlačení reakcí. Ty by totiž mohly útočníkovi poskytovat zpětnou vazbu. Je nezbytné útočníka zablokovat na všech platformách, aby neměl možnost zkontaktovat oběť i prostřednictvím další platformy. Ačkoliv se oběť může cítit ponížena nebo vystrašena, neměla by čelit situaci sama. Velký důraz je kladen na uchovávání důkazů ze zpráv, e-mailů a chatů, které mohou posloužit jako podklad pro vyšetřování a následně také podpora oběti

(Jak se chránit před kyberšikanou a jak se bránit kyberútočníkům, 2009). Té byla věnována předchozí podpodkapitola.

Pokud by u sextingu došlo k rozeslání fotek oběti nebo dokonce vložení na sociální síť, je důležité zachovat klid. Při vydírání se doporučuje nereagovat na zprávu nebo alespoň odpovídat zdvořile a slovně neútočit. Lze se například vymluvit na domácí či školní povinnosti a utéct tak z konverzace. Nejdůležitější je hlavně nesmazat veškerou konverzaci s útočníkem a říct o svém problému důvěryhodné osobě nebo kontaktovat online poradnu (Vohanková, 2020).

3.4.3 Obnovení bezpečnosti

Na základě poznatků ohledně prevence, které byly uvedeny výše, vyplynula důležitost pravidelné péče o své zařízení a aktualizaci bezpečnosti. Opatření, jako je instalace antivirových programů nebo dodržování daných pravidel pohybu na internetu, nejsou pouze doporučeními, ale nezbytnými kroky pro minimalizaci rizik online útoků. I přes dostupné nástroje pro ochranu je i tak nutné být obezřetný. K zajištění bezpečnosti v digitálním světě je potřeba se nespoléhat jen na technologie, ale také věnovat pozornost svému chování a návykům.

II PRAKTICKÁ ČÁST

4 VÝZKUM

Internet nabízí mladým lidem rozsáhlé možnosti. Ty jsou jak pozitivní, tak negativní. Někteří mladí lidé mohou být ohroženi online riziky, jako jsou například kybergrooming, kyberšikana, nevhodný obsah a další (Whittle et al., 2013). Během posledních 10 let došlo zásadním změnám v užívání a způsobu využití digitálních technologií mladými lidmi, kteří své chytré telefony využívají každý den, a to téměř dvakrát více než před 10 lety. Také je využívají od mnohem mladšího věku. Moderní zařízení jim umožňují komunikovat s ostatními, učit se online a bavit se, přičemž to nese svá rizika, jako je nebezpečí vystavení dezinformacím, kyberšikaně nebo škodlivému a nezákonnému obsahu (Smahel et al., 2020).

Porozumění jejich názorům a jejich vnímání bezpečnosti je zásadní pro navrhování účinných preventivních opatření a ochranných strategií. Tato bakalářská práce se proto zaměřuje na studii faktorů, které ovlivňují vnímání a řešení rizik online prostředí u pubescentů. Pozornost byla věnována především jejich postojům v této problematice. Konkrétně tedy jak bezpečnost v digitálním světě vnímají oni sami. Kromě postojů žáků byly zkoumány prožité zkušenosti žáků v digitálním světě a je jejich prevence vůči rizikům digitálního světa (například obtěžování, kyberšikana atd.).

Studie *Porozumění zkušenostem mládeže v USA s digitální bezpečností z roku 2023* se zaměřuje na útoky, kterým mladí lidé čelí, a jejich vzájemnou propojenost napříč digitálními platformami i fyzickým světem. Autoři zjistili, že tyto útoky, včetně kyberšikany a sexuálního násilí, se často stupňují a ovlivňují emocionální a fyzickou bezpečnost mládeže. Mládež se setkává s různými hrozbami, jako jsou toxické komentáře, vydávání se za někoho jiného a výhrůžky, které mohou vést k psychickému i fyzickému poškození. Mnoho mladých lidí čelí krádeži identity a sexuálnímu násilí, které může mít vážné důsledky včetně emočního traumatu. K prevenci těchto útoků mládež využívá různé strategie, jako je sledování aktivit, omezení přístupu na platformy a oznamování útoků. Avšak nedostatek vzdělání o digitální bezpečnosti a neochota sdílet obavy s dospělými vedou k tomu, že se mladí lidé cítí méně chráněni. Studie zdůrazňuje potřebu vytvoření koordinovaného ekosystému digitální bezpečnosti, který respektuje autonomii mladých lidí a zahrnuje všechny zainteresované strany. Cílem tohoto výzkumu je zlepšit ochranu mládeže a lépe integrovat jejich hlasy do diskuse o digitální bezpečnosti (Freed et al., 2023).

Szotkowski et al. (2013) se ve své studii *Nebezpečí internetové komunikace IV* zabývají rizikovým chováním českých dětí na internetu. Celkový počet respondentů byl

21 372 a věkové ohraničení bylo od 11 do 17 let. Zaměřují se především na kyberšikanu, sexting, internetové seznamování, vnímání pravdy a lži a další. Studie odhalila, že téměř polovina dětí byla obětí kyberšikany a přibližně 30 % dětí se stalo útočníky. Více než polovina (53 %) dětí komunikuje s lidmi na internetu, i přesto že je neznají a více než 26 % si přidá cizí osobu mezi své přátele na sociálních sítích. Autoři studie také zjistili, že přes 49 % dětí šlo na schůzku s člověkem, kterého neznají. V oblasti sextingu zjistili, že 7,23 % sdílí sexuálně laděný materiál na internet a téměř 9 % odesílá vlastní sexuální materiál jiným osobám. Při sdílení osobních údajů nejčastěji děti sdílí jméno a příjmení, dále e-mail, fotografii svého obličeje a o něco méně dětí sdílí své telefonní číslo, adresu školy nebo svého bydliště. Minimum dětí sdílí své rodné číslo, heslo k e-mail účtu a PIN kreditní karty.

Hykyšová (2019) ve svém výzkumu *České děti se chodí na internet bavit* zjistila, že děti od 9 do 17 let komunikují s lidmi, které neznají osobně, a to přibližně polovina z dotazovaných. S osobním setkáním souhlasilo (a také přišlo) téměř polovina.

4.1 Výzkumné cíle

Hlavním výzkumným cílem je **analyzovat pohled pubescentů na bezpečnost v digitálním světě**.

Dále byly zvoleny dílčí výzkumné cíle:

- 1) Identifikovat typy digitálních rizik, které jsou pubescentům známe.
- 2) Analyzovat zkušenosti pubescentů s digitálními riziky.
- 3) Analyzovat pocity pubescentů při setkání s digitálními riziky.
- 4) Analyzovat strategie, které pubescenti používají k prevenci rizik spojených s používáním digitálních technologií.

4.2 Výzkumné otázky

Hlavní výzkumná otázka zní: **Jaký je pohled pubescentů na bezpečnost v digitálním světě?**

Jako dílčí výzkumné otázky byly zvoleny následující:

D.V.O.1: Jaké typy digitálních rizik jsou pubescentům nejvíce známe?

D.V.O.2: Jaké jsou zkušenosti pubescentů s digitálními riziky při užívání online prostředí?

D.V.O.3: Jaké jsou pocity pubescentů při setkání s těmito riziky?

D.V.O.4: Jaké strategie užívají pubescenti v prevenci rizik spojených s používáním digitálních technologií?

4.3 Druh výzkumu

Pro zpracování praktické části byl zvolen kvantitativní výzkum, který je dle Chrásky (2016, s. 158) výhodný zejména z toho důvodu, že „umožňuje poměrně rychlé a ekonomické shromažďování dat od velkého počtu respondentů.“ Kvantitativní výzkum umožnil zkoumat širší spektrum pohledů a zkušeností pubescentů, což je klíčové k pochopení jejich postojů k bezpečnosti v digitálním světě. Druh výzkumu byl také zvolen v souladu s výzkumnými cíli a otázkami, které se zaměřují na pohled, zkušenosti, pocity a prevenci pubescentů v digitálním světě. Výzkum byl prováděn pomocí dotazníkového šetření.

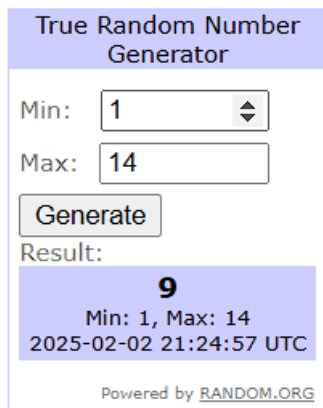
4.4 Výzkumný soubor

Základním souborem výzkumu byli pubescenti od věku 11 až 15 let. Tato věková skupina byla vybrána s ohledem na téma této práce. Pubescenti představují populaci, která aktivně využívá digitální technologie a zároveň je ve zvýšené míře vystavena rizikům spojených s digitálním prostředím (Redakce Radinet.cz, 2024).

Výběrový soubor tvoří pubescenti ve věku od 11 do 15 let ze základních škol a gymnázií. Dotazník byl distribuován elektronicky, aby byla zajištěna efektivní dostupnost a větší počet získaných odpovědí. Pro tento výzkum byl zvolen prostý náhodný výběr, při kterém byla dle Chrásky (2016) přiřazena jednotlivým krajům ČR čísla (Tabulka 1), která byla následně náhodně vylosována.

Tabulka 1 Seznam krajů dle čísel

1	Hlavní město Praha	6	Královehradecký kraj	11	Plzeňský kraj
2	Jihočeský kraj	7	Liberecký kraj	12	Středočeský kraj
3	Jihomoravský kraj	8	Moravskoslezský kraj	13	Ústecký kraj
4	Karlovarský kraj	9	Olomoucký kraj	14	Zlínský kraj
5	Kraj Vysočina	10	Pardubický kraj		



True Random Number Generator

Min:

Max:

Result:

9

Min: 1, Max: 14
2025-02-02 21:24:57 UTC

Powered by RANDOM.ORG

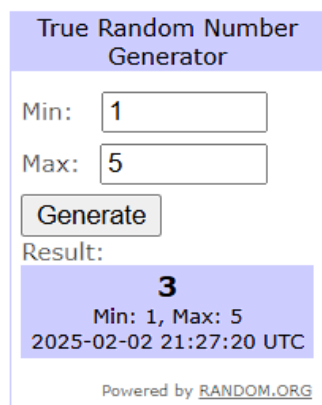
Obrázek 2 Losování kraje

(zdroj: vlastní)

Dále proběhlo také losování okresu, při kterém byl použit stejný nástroj, tzn. že okresy byly seřazeny také dle abecedy a podle toho také číselně (Tabulka 2). Při losování bylo vygenerováno číslo 3, tedy okres Prostějov (Obrázek 3).

Tabulka 2 Seznam okresů Olomouckého kraje dle čísel

1	Jeseník
2	Olomouc
3	Prostějov
4	Přerov
5	Šumperk



True Random Number Generator

Min:

Max:

Result:

3

Min: 1, Max: 5
2025-02-02 21:27:20 UTC

Powered by RANDOM.ORG

Obrázek 3 Losování okresu

(zdroj: vlastní)

V dalším kroku byly náhodně losovány konkrétní školy. Vždy bylo vylosováno náhodné číslo a oslovena škola. Z důvodu časové efektivity byl osloven širší okruh škol. Ze seznamu škol byly vyloučeny základní školy, které poskytují pouze 1. stupeň základního

vzdělávání. Osloveno bylo celkem sedmnáct škol, z nichž se spoluprací souhlasily tři. Škol se však mohlo zapojit více, ale nebyla vrácena zpětná vazba. V případě jedné školy byla až po opětovné žádosti zpětná vazba vrácena se sdělením, že dotazník byl již žákům dán.

Respondenti byli osloveni prostřednictvím své školy. Jak bylo již zmíněno, nejdříve byly osloveny základní školy a gymnázia s prosbou o distribuci dotazníku. Žákům byl poskytnut prostor na počítačích, popřípadě bylo možné dotazník vyplnit i na mobilním telefonu. Toto rozhodnutí bylo na samotné škole. Zároveň byla také ponechána možnost pouhého sdílení dotazníku skrze školní e-mail či jiné platformy využívané ke komunikaci mezi školou, žáky a popřípadě rodiči.

4.5 Metoda výzkumu

Pro získání potřebných dat bylo zvoleno online dotazníkové šetření. Dotazník byl vytvořen a distribuován pomocí internetu skrze platformu Google Forms. Respondenti byli na začátku dotazníku informováni o účelu dotazníku a zároveň jim byla slíbena také anonymita.

Dotazník je zaměřen na zkušenosti pubescentů s různými typy rizik, konkrétně, zda sám respondent zažil setkání s rizikem, zda zná někoho, kdo se s rizikem setkal nebo zda sám byl iniciátorem rizika. Dále také na jejich pocity při setkání a prevenci vůči rizikům. Dotazník byl navržen tak, aby na základě šetření bylo možné zodpovědět výzkumné otázky a naplnit výzkumné cíle. Je členěn několika tematických částí, které odpovídají jednotlivým výzkumným otázkám. Následně byly položky logicky seřazeny tak, aby byla podobná témata seřazena za sebou sebe, včetně typů rizik. Stejným způsobem jsou řazeny otázky zaměřené na pocity, které pubescenti prožívají při setkání se zmíněnými riziky.

Dotazník obsahuje uzavřené nebo polootevřené položky, přičemž nejvíce bylo polootevřených otázek. Uzavřené neboli strukturované položky se charakterizují předložením již připravených odpovědí, ze kterých si respondent vybírá, u polouzavřených položek je rozšířena nabídka odpovědí o odpověď „jiná odpověď“. Jediná položka byla otevřená a týkala se věku respondenta, kdy každý respondent napsal svůj věk (Chrásková, 2016).

Jak již bylo zmíněno ve druhé kapitole, rizika na internetu byla vybrána na základě Projektu E-Bezpečí (Informace o projektu - E-bezpečí, c2008-2024), přičemž tento výzkum je zaměřen právě na tato, protože jsou projektem považovány za nejzávažnější. V dotazníku byla také použita typologie emocí dle Golemana (2011), která byla použita pro zodpovězení

třetí dílčí výzkumné otázky a zaměřuje se na pocity při setkání s daným rizikem (viz 2.7). Rizika i emoce byly tedy zakomponovány do dotazníku.

Vzhledem k nastaveným cílům byl vytvořen dotazník vlastní konstrukce a zahrnul všechna rizika, která byla definována v teoretické části práce. Pro inspiraci byly využity dva dotazníky, a to konkrétně od Bc. Šárky Holcové, která se ve své diplomové práci zaměřuje na formy rizikového chování adolescentů na internetu (Holcová, 2019), a z výzkumu EU Kids Online 2020 (Smahel, 2020). Tyto dva výzkumy poskytly základ a inspiraci pro formulaci položek dotazníku. Existují také dotazníky zaměřující se konkrétně na dílčí rizika, např. v diplomové práci Bc. Davida Špeldy, která se zabývá zmapováním problému kyberšikany a zkoumá znalosti a postoje žáků tohoto problému (Špelda, 2020).

4.6 Způsob zpracování dat

Ke zpracování dat byla opět využita platforma Google Forms, která je zdarma dostupná na internetu. Umožňuje zpracování a analýzu získaných odpovědí do přehledných grafů a tabulek po ukončení sběru dat. Ty lze následně převést do tabulky editované v programu Excel, se kterou bylo nadále pracováno. Dotazník je uveden v přílohách této práce (Příloha P I: Dotazník).

4.7 Limity výzkumu

Limity tohoto výzkumu zahrnují menší vzorek respondentů, což mohlo ovlivnit zobecnitelnost výsledků na populaci. Pro zajištění vyšší reprezentativnosti by bylo vhodnější zajistit větší počet respondentů. Dalším limitem by mohla být délka dotazníku, která mohla ovlivnit ochotu a vytrvalost respondentů dokončit celý dotazník. Tato délka ale byla nezbytná, jelikož zahrnuje širokou škálu rizik dle zmíněné typologie, která byla klíčová pro komplexnímu pochopení této problematiky.

5 ANALÝZA

Na úvod je třeba říci, že u každé odpovědi bude vypsána relativní četnost odpovědí, u položek zaměřených na pocity při setkání s riziky bude také uvedena stěžejní emoce, která danou odpověď vystihuje, popřípadě její dílčí emoci. Ne vždy jsou uvedeny všechny emoce, a to hlavně ty pozitivní, jelikož to u některých položek nebylo zcela možné. Pod některými jsou také přiloženy grafy s procentuální četností. Analýza položek je rozdělena dle dílčích výzkumných otázek a na začátku samozřejmě obecné informace o pubescentech. Pro přehled byla také vytvořena tabulka s položkami pod konkrétními výzkumnými otázkami, lze ji nalézt v přílohách této práce (Příloha P 2: Položky v dotazníku a výzkumné otázky).

1) Pohlaví

První položka se dotazovala na pohlaví pubescentů. Celkový počet byl 284 pubescentů, z toho bylo 153 dívek a 131 chlapců. V procentech lze hovořit o 53,87 % za dívky a 46,13 % za chlapce.

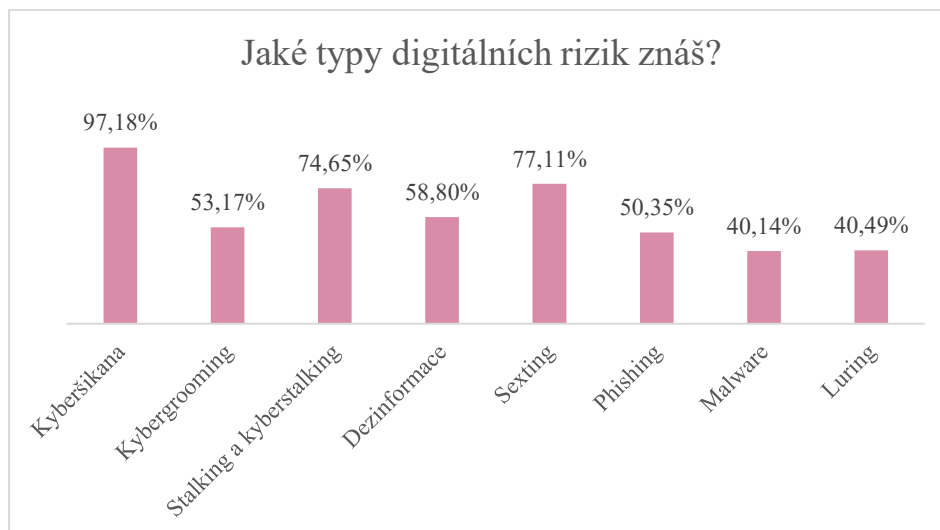
2) Kolik je ti let?

Druhá položka zjišťovala věk pubescentů, přičemž nejméně bylo jedenáctiletých, konkrétně 17 pubescentů neboli 5,99 %. Dvanáctiletých tvořilo 20,77 % a bylo jich celkem 59. Největší část tvořili třináctiletí pubescenti, přičemž jich bylo 75, což je 26,41 %. O něco méně bylo čtrnáctiletých, těch bylo 69, respektive 24,30 %. Těch nestarších, kteří měli patnáct let bylo 22,54 % a bylo jich 64.

5.1 Jaké typy digitálních rizik jsou pubescentům nejvíce známé?

3) Jaké typy digitálních rizik znáš?

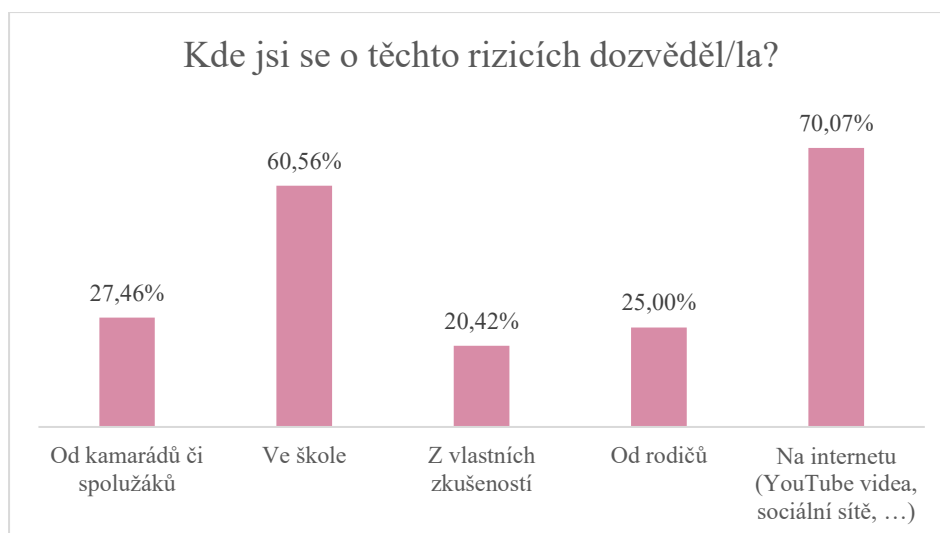
Ve třetí položce byla zjišťována znalost pubescentů, co se týče rizik v digitálním světě. Ke každé odpovědi byla připsána i definice termínu. Předpokládalo se totiž, že pubescent může dané riziko znát, aniž by si vybavil přesný název. V grafu níže (Graf 1) si lze všimnout, že nejznámějším rizikem mezi pubescenty je kyberšikana, kterou zná 97,18 % z nich. Následuje sexting, o kterém ví 77,11 % pubescentů. Stalking a kyberstalking je známý 74,65 % dotazovaným, zatímco dezinformace zná 58,80 %. O kybergroomingu má povědomí 53,17 % a o phishingu ví 50,35 %. Nejméně známým rizikem je luring s 40,49 % a trochu méně malware s 40,14 %. V možnosti „Jiná“ byly uvedeny další dvě rizika – skimming a bluewhale challenge.



Graf 1 Znalost rizik

4) Kde jsi se o těchto rizicích dozvěděl/a?

Dále čtvrtá položka, která se zaměřuje na místo nebo osobu, kde se o zmíněných rizicích dozvěděl. Při pohledu na graf (Graf 2) lze říci, že o rizicích se pubescenti dozvídají nejvíce z internetu, a to konkrétně 70,07 % z nich. O něco méně pak ve škole a tedy 60,56 %. Od kamarádů či spolužáků se dozvídá pouze 27,46 %, od rodičů přesných 25 % a nejméně čerpají z vlastních zkušeností, a to konkrétně 20,42 %. Mimo to také uváděli zdroj informací o rizicích na internetu televizi, školní přednášku, sestru (lze tedy brát obecně jako sourozence) a dva lidé paní učitelku.



Graf 2 Zdroj informací o rizicích

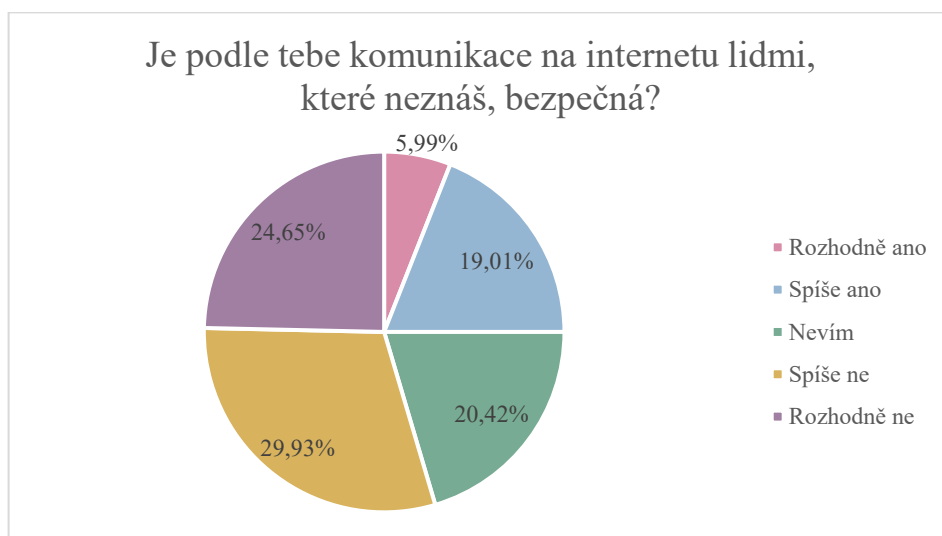
5.2 Jaké jsou zkušenosti pubescentů s digitálními riziky při užívání online prostředí?

5) Chováš se na internetu bezpečně?

Pátá položka se dotazovala na pubescentův pohled na své chování na internetu, respektive zda považuje své chování za bezpečné. Velká většina pubescentů, konkrétně 91,55 %, považuje své chování na internetu za bezpečné a pouhých 8,45 % ho vnímá naopak.

7) Je podle tebe komunikace na internetu lidmi, které neznáš, bezpečná?

V sedmé položce byli pubescenti dotazováni, zda vnímají komunikaci s cizími lidmi jako bezpečnou či nikoliv. Opět měli možnost od rozhodně ano až po rozhodně ne, tentokrát byla na výběr také odpověď „nevím“. Nejčastější odpověď je „spíše ne,“ přičemž si ji vybralo 29,93 % pubescentů. 24,65 % vnímá komunikaci s cizími lidmi na internetu jako naprosto nebezpečnou. Již zmíněnou neutrální odpověď „nevím“ zakliklo 20,42 % odpovídajících. 19,01 % tvrdí, že je komunikace s cizími lidmi na internetu spíše bezpečná a nejméně z nich a 5,99 %, ji vnímá jako naprosto bezpečnou.



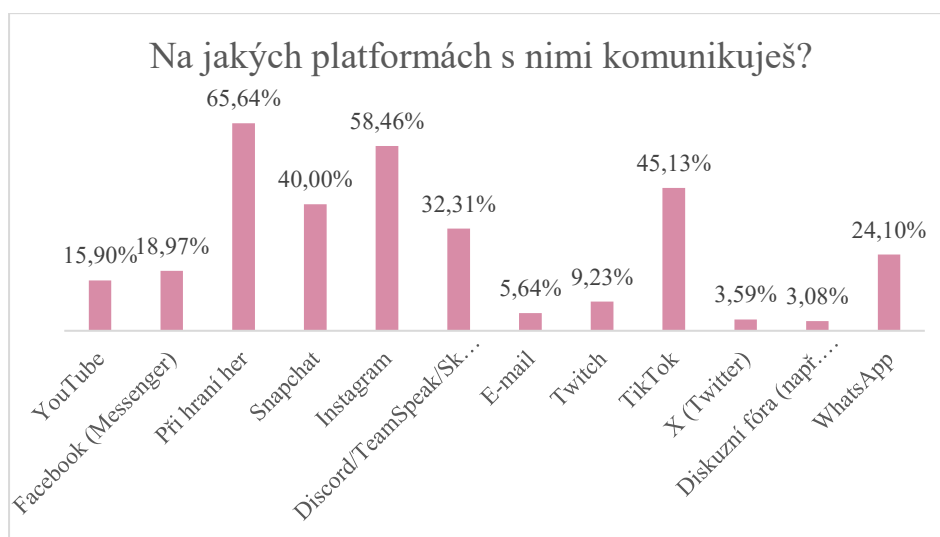
Graf 3 Vnímání komunikace s cizími lidmi na internetu

8) Komunikuješ na internetu s lidmi, které neznáš? (např. na sociálních sítích, při hraní her)

Osmá položka se byla zaměřena se na to, zda pubescenti komunikují s cizími lidmi na internetu. Většina z nich, konkrétně 68,66 %, uvedla, že s cizími lidmi komunikuje, naopak 31,34 % s nimi nekomunikuje.

9) Na jakých platformách s nimi komunikuješ?

Devátá položka navazuje na tu předchozí, a proto bude počítáno se 195 pubescenty. Dotazuje se, na kterých platformách, respektive sociálních sítích, počítačových hrách a dalších, s nimi navazují kontakt (Graf 4). Na výběr měli mnoho možností, ale nejvíce uváděli, že komunikují s cizími lidmi při hraní her, a to konkrétně 65,64 % z nich. O něco méně, 58,46 %, s nimi komunikuje na sociální síti Instagram, 45,13 % na TikToku a 40 % na Snapchatu. Skrze digitální hlasovou, textovou nebo video komunikaci (Discord, TeamSpeak, Skype) s cizími lidmi komunikuje 32,31 %. Na platformě WhatsApp s nimi komunikuje 24,10 %. Dále 18,97 % dotazovaných k této komunikaci využívá sociální síť Facebook, respektive Messenger, dalších 15,90 % z nich YouTube, 9,23 % Twitch, 5,64 % E-mail a 3,59 % sociální síť X (dříve Twitter). Nejméně pubescentů, 3,08 %, navazuje komunikaci na diskusních fórech jako je například Reddit. Dále pubescenti uvedli Omegle, Telegram, Roblox, VRchat a Minecraft. Roblox (3 odpovědi) a Minecraft (1 odpověď) lze zahrnout do kategorie hraní her, přičemž tyto dvě jsou už konkrétní počítačové hry. Hned osm dotazovaných napsalo odpověď Telegram a jeden pubescent také uvedl VRchat.



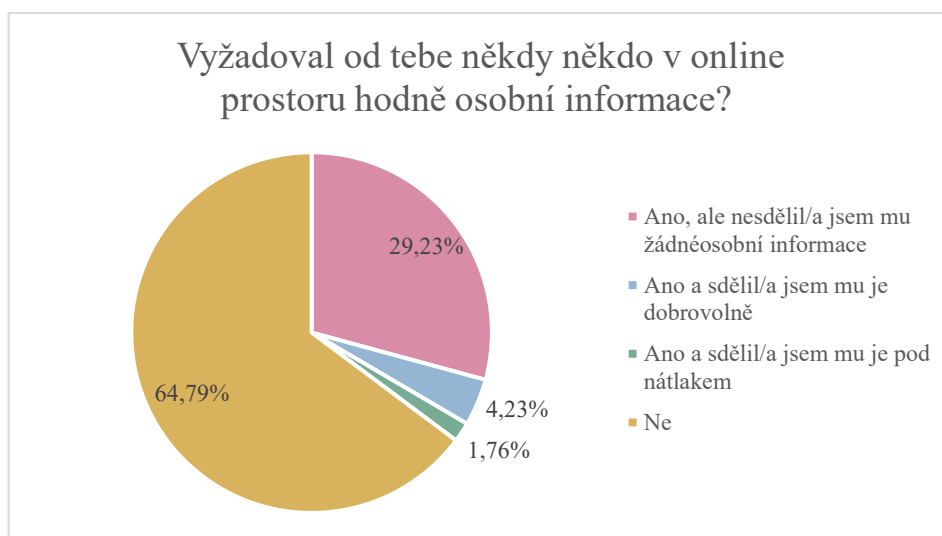
Graf 4 Platformy pro komunikaci s cizími lidmi

10) Setkal/a jsi se někdy s někým v online prostoru, kdo ti psal hodně osobní zprávy?

Desátá položka je zaměřena na digitální riziko kybergroomingu. Konkrétně se dotazovala, zda se někdy za svůj život setkali s osobou na internetu, která jim psala až příliš osobní zprávy o sobě samém. 66,90 % respondentů se s tím nikdy nesetkalo, naopak 33,10 % ano.

11) Vyžadoval od tebe někdy někdo v online prostoru hodně osobní informace?

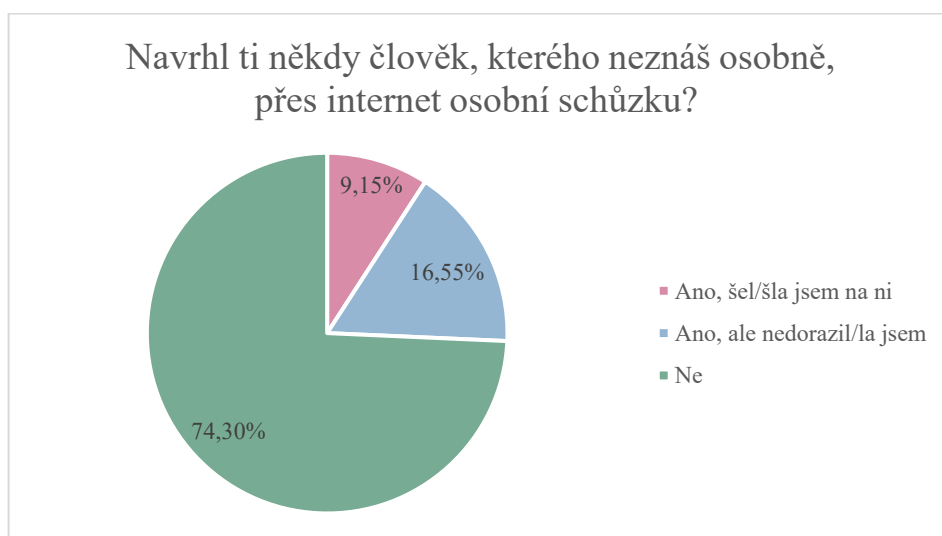
Jedenáctá položka navazuje na předchozí, jelikož se ptá pubescenta, zda naopak od něj někdo vyžadoval tyto informace (Graf 5), přičemž 64,79 % se s tímto jevem nesetkalo. 29,23 % takovou situaci zažilo, ale dané osobě žádné informace nesdělilo. Dále 4,23 %, které jim naopak své citlivé informace sdělilo dobrovolně a 1,76 % pod nátlakem či manipulací.



Graf 5 Vyžadování osobních informací cizím člověkem

12) Navrhl ti někdy člověk, kterého neznáš osobně, přes internet osobní schůzku?

Ve dvanácté položce byli pubescenti dotazováni, zda jim někdo někdy navrhl osobní schůzku (Graf 6), přičemž 9,15 % dotazovaných se schůzkou souhlasilo a také na ni dorazilo. Dále 16,55 % pubescentů se do této situace dostalo, ale na schůzku nedorazilo. Velké většině, konkrétně 74,30 %, se nic takového nestalo.



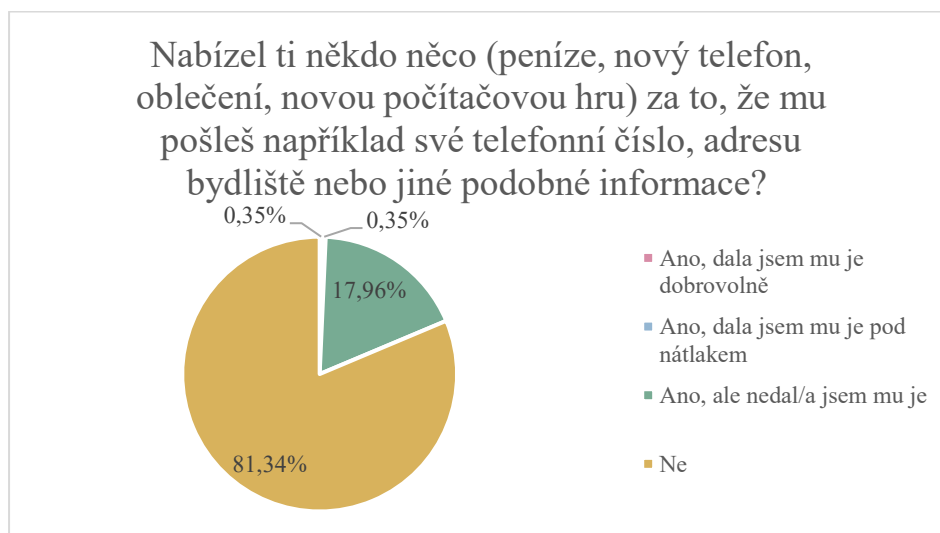
Graf 6 Návrh osobní schůzky

13) Napsal ti někdy někdo cizí na internetu podobnou zprávu? „neříkej to rodičům, nepochopí to“ nebo „pokud jim to prozradíš, budeš mít problémy“

Třináctá položka se zaměřuje na techniku kybergroomingu – izolace oběti (viz 2.2.6). S tímto rizikem se setkalo 8,80 % dotazovaných.

14) Nabízel ti někdo něco (peníze, nový telefon, oblečení, novou počítačovou hru) za to, že mu pošleš například své telefonní číslo, adresu bydliště nebo jiné podobné informace?

Čtrnáctá položka se zaměřuje na riziko luringu (viz 2.2.4). Podle grafu níže (Graf 7) lze říci, že většina pubescentů, 81,34 %, se s tímto rizikem vůbec nesetkala. Naopak 17,96 % z nich ano, přičemž manipulaci nepodlehli a požadované informace útočníkovi neposkytli. Jeden dotazovaný pubescent (0,35 %) bohužel manipulaci podlehl a pod nátlakem mu informace sdělil, jiný (0,35 %) tyto informace poskytl dobrovolně.



Graf 7 Luring

16) Přišel ti někdy e-mail, který se ti zdál podezřelý? (byl od cizí osoby, zvláštní text, obsahoval odkaz)

V šestnácté položce byli pubescenti dotazováni, zda jim někdy přišel e-mail, který obsahoval phishing (viz 2.2.2). Kromě nabídky odpovědi ano či ne, měli možnost si vybrat odpověď neutrální, přičemž si nevybavují nebo nepamatují, zda se s tím setkali nebo ne. Konkrétně tedy 39,44 % dotazovaných tento e-mail přišel, 40,85 % naopak ne. 19,72 % pubescentů si informaci v danou chvíli nevybavilo.

18) Klikl/a jsi někdy na odkaz, který ti přišel od kohokoliv, přitom jsi nevěděl/a, co se v odkaze nachází?

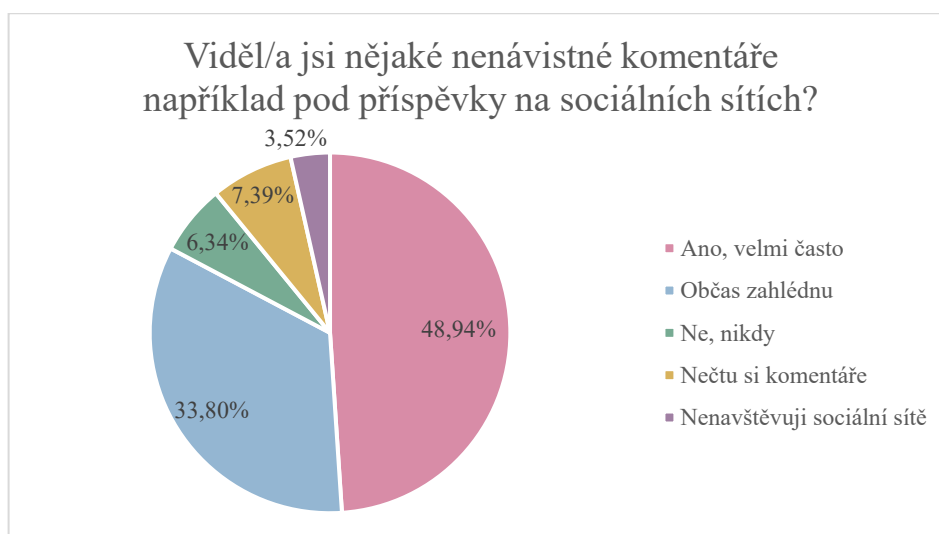
Následovala osmnáctá položka, která se opět týká phishingu, a to konkrétně opatrnosti pubescentů. I přesto, že se může jednat o jejich blízkého kamaráda, existuje zde pravděpodobnost, že se někdo dostal na jeho účet a rozesílá nebezpečné odkazy. Omylem na odkaz kliklo 24,65 %, úmyslně 12,32 % a nikdy 63,03 %.

19) Podařilo se ti někdy omylem stáhnout nějaký druh malwaru? (např. virus, trojský kůň, adware atd.)

Devatenáctá položka svým způsobem nepřímo navazuje také na předchozí položku. Malware lze nechtěně stáhnout i jiným způsobem než jen při phishing útoku. 57,39 % pubescentů se nikdy nepodařilo omylem stáhnout jakýkoliv druh malwaru, 19,01 % z nich neví nebo si to nepamatují nevybavují, ale připouští možnost, že se jim to někdy stalo, a 23,59 % se to naopak opravdu někdy stalo.

21) Viděl/a jsi nějaké nenávistné komentáře například pod příspěvky na sociálních sítích?

Ve dvacáté první položce byli pubescenti dotazováni, zda viděli nějaké nenávistné komentáře na sociálních sítích. Položka se zaměřuje na riziko kyberšikany skrze psaní nenávistných a urážejících komentářů. Graf níže (Graf 8) ukazuje, že 48,94 % z nich je vidí velmi často, 33,80 % je zahlédne jen občas a 6,34 % tvrdí, že je nikdy nevidělo. Dále 7,39 % uvádí, že si nečtou komentáře a 3,52 % ani nenavštěvuje sociální sítě.



Graf 8 Nepřímé setkání s nenávistnými komentáři

22) Přišel ti někdy nenávistný komentář pod tvůj příspěvek? (fotka či video na sociálních sítích)

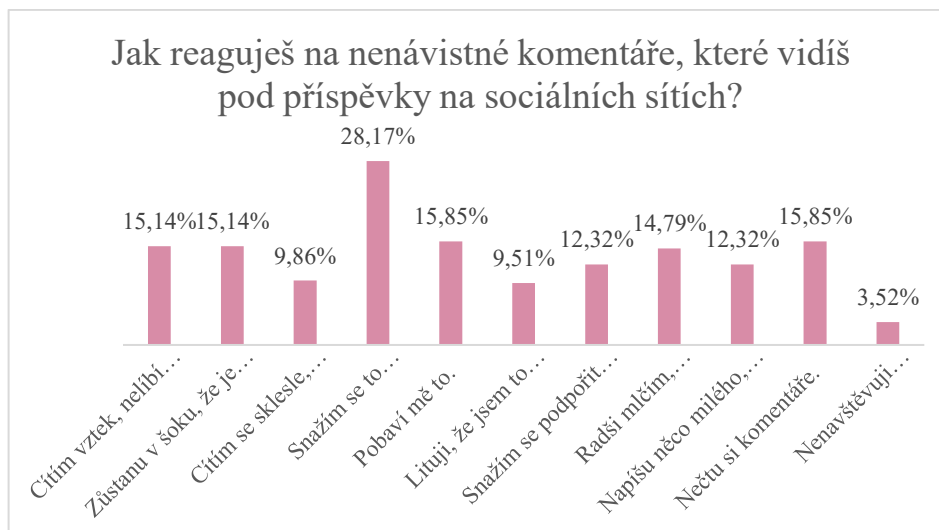
Dvacátá druhá položka se pojí s předchozí a dotazuje se, zda pubescentovi samému přišel někdy takový komentář pod jeho příspěvek. Včetně 3,52 % z nich, kteří nenavštěvují sociální síť, se s tímto nesetkalo 64,44 % a 32,04 % ano.

23) Napsal/a jsi ty někdy takový komentář?

Dvacátá třetí položka se dále ptá, zda pubescent sám napsal takový komentář, kde je opět 3,52 %, kteří nenavštěvují sociální síť. 68,66 % z celku uvedlo, že nikoliv a 27,82 % tento komentář někdy napsalo.

24) Jak reaguješ na nenávistné komentáře, které vidíš pod příspěvky na sociálních sítích?

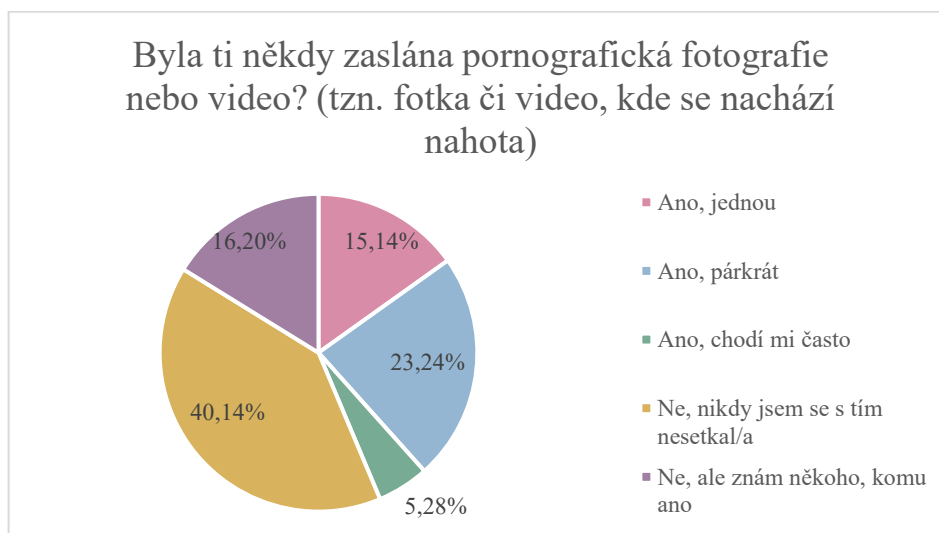
Dvacátá čtvrtá položka se zaměřuje na reakci na nenávistné komentáře, přičemž zahrnuje i některé z emocí a zároveň konkrétní možné reakce a možnost napsání své vlastní odpovědi, výsledky lze vidět na níže uvedeném grafu (Graf 9). Opět zde byla zahrnuta možnost odpovědi, že nenavštěvují sociální síť, tedy 3,52 %. Nejhojněji byla vybírána neutrální odpověď, konkrétně 28,17 %, přičemž se tedy snaží komentáře ignorovat a neřešit je. Dále 15,85 % se cítí pobaveně, zde lze přiřadit emoci radost, a stejné procento uvedlo, že si komentáře nečte. To sice neodpovídá s dvacátou první položkou, ale nabízí se domněnka, že si těchto komentářů všímají, ale podrobně si je nečtou. Dále 15,14 % pubescentů, kteří cítí vztek, kde lze přiřadit emoci hněv a podkategorii rozhořčenost. Zároveň se stejným procentem odpovědí je emoce překvapení, kde je dílčí emoce šok a pubescenti se cítí v šoku, že je někdo tak „zlý“. Reakce se zdržuje 14,79 %, jelikož nechtějí být terčem dalších útoků. Naopak 12,32 % se snaží podpořit oběť nenávistných komentářů a dalších 12,32 % napíše nějaký milý komentář, aby vyvážili negativitu v komentářích. Dále 9,86 % se cítí sklesle, což lze přiřadit k emoci smutek a podkategorii sklíčenost, v odpovědi je dále zmíněno, že jim to kazí náladu. 9,51 % lituje, že daný komentář vůbec přečetlo, lze tedy říci, že cítí emoci hanbu, kde je dílčí emoce lítost. Nad rámec již určených odpovědí se vyskytovaly odpovědi, že je to pubescentům jedno (3 odpovědi). Jeden pubescent uvedl, že se cítí zle „když to někdo někomu napíše jen tak,“ jeden respondent komentář nahlásí. Dva se dokonce údajně k nenávistným komentářům přidají. Dalšímu záleží, zda autor nenávistného komentáře má pravdu, nebo řeší hlouposti. Poslední odpověď zněla takto: „Někdo si nejspíš myslí, že sám je dokonalý, tak si musí někde zvyšovat ego.“



Graf 9 Reakce na nenávistné komentáře

26) Byla ti někdy zaslána pornografická fotografie nebo video? (tzn. fotka či video, kde se nachází nahota)

Dvacátá šestá položka naráží na sexting (viz 2.2.5). Konkrétní výsledky ukazují (Graf 10), že 40,14 % pubescentů se s tím vůbec nesetkalo. Dále 16,20 % uvádí, že se s tím nesetkali, ale znají někoho, kdo ano. 15,14 % takový materiál alespoň jednou přišel, 23,24 % více jak jednou (párkrát) a 5,28 % chodí často.

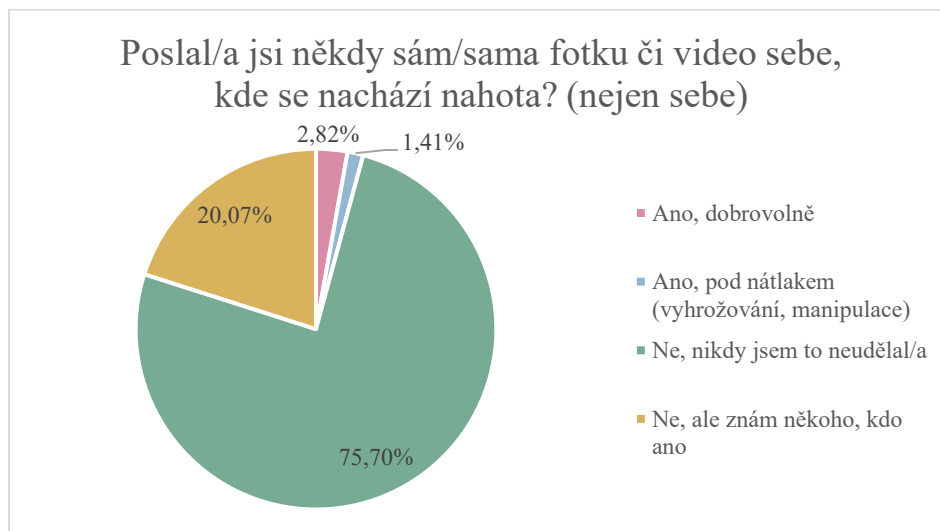


Graf 10 Příjem pornografického materiálu

28) Poslal/a jsi někdy sám/sama fotku či video sebe, kde se nachází nahota? (nejen sebe)

Dvacátá osmá položka dále navazuje na předchozí a dotazuje se, zda pubescenti samotní poslali fotku s nahotou (Graf 11). Nemusí jít o fotografii sebe samého, ale může se jednat i o přeposílání, respektive šíření tohoto materiálu, přičemž 75,70 % pubescentů se toho nikdy

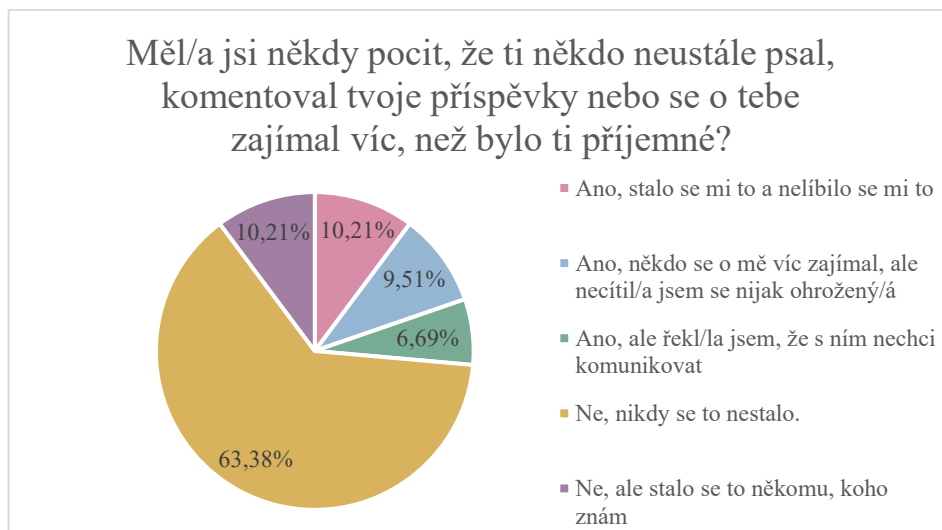
nedopustilo. Dále 20,07 % osobně ne, ale znají někoho, kdo fotky či videa poslal někomu dalšímu. 2,82 % je poslali dobrovolně a 1,41 % podlehl nátlaku, vyhrožování nebo manipulaci a materiál osobě poslali.



Graf 11 Šíření (vlastního) pornografického materiálu

29) Měl/a jsi někdy pocit, že ti někdo neustále psal, komentoval tvoje příspěvky nebo se o tebe zajímal víc, než bylo ti příjemné?

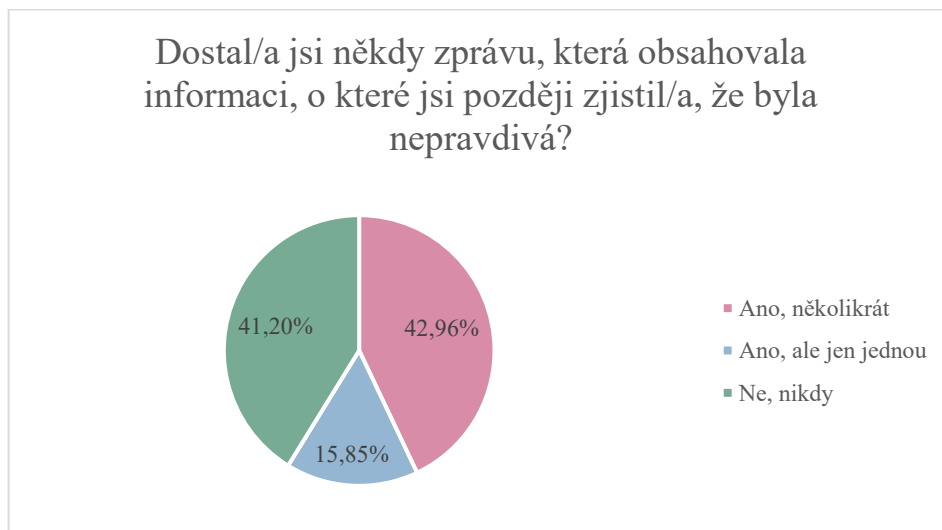
Dvacátá devátá položka se dotýká oblasti stalkingu a především kyberstalkingu (viz 2.3). Z grafu vyplývá (Graf 12), že 63,38 % pubescentů toto chování nikdy nezaznamenalo, 10,21 % totéž, přičemž zná ve svém okolí někoho, kdo ano. To může ukazovat další rozšířenost tohoto rizika. Dalších 10,21 % říká, že se jim to stalo a toto chování nelíbilo se jim. Dále 9,51 % pubescentů, kteří si nepřipadali nijak ohrožení. Lze tedy předpokládat, že riziko rozpoznali. Zbývajících 6,69 % setkání řešilo vyjádřením nezájmu o další komunikaci.



Graf 12 Nadměrný zájem a kontrola jiným uživatelem

31) Dostal/a jsi někdy zprávu, která obsahovala informaci, o které jsi později zjistil/a, že byla nepravdivá?

Třicátá první položka zjišťovala výskyt dezinformací (viz 2.5), respektive jejich příjem u pubescentů. Z níže uvedeného grafu (Graf 13) lze říci, že 42,96 % dotazovaných takovou zprávu již několikrát zaznamenalo, 41,2 % pubescentů nikdy a 15,85 % alespoň jednou.

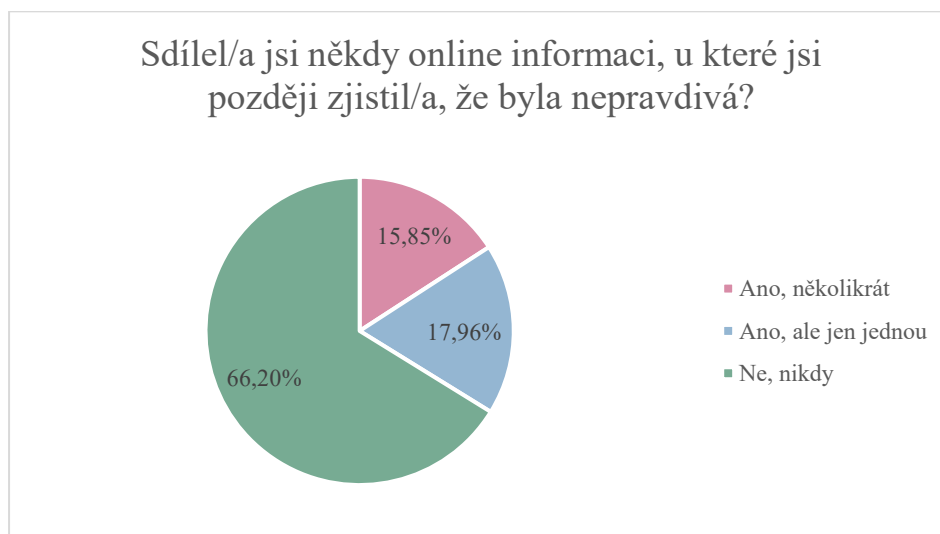


Graf 13 Výskyt dezinformací

33) Sdílel/a jsi někdy online informaci, u které jsi později zjistil/a, že byla nepravdivá?

Dále třicátá třetí položka, která se dotazuje na to, zda sami pubescenti šířili nějakou dezinformaci. Může se jednat o příchozí zprávu, článek na internetu či příspěvek na sociálních sítích, přičemž níže uvedený graf (Graf 14) ukazuje, že 66,2 % nikdy

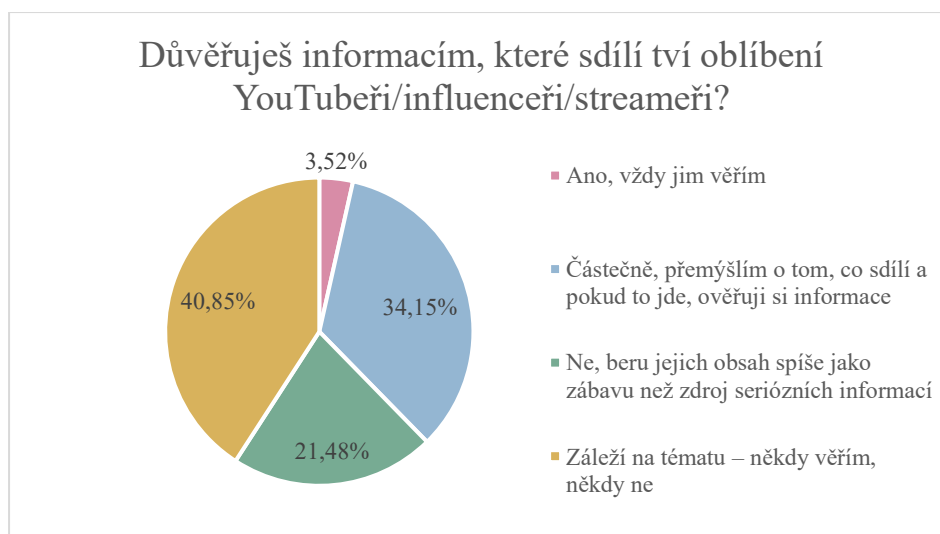
dezinformaci nešířilo. 17,96 % tvrdí opak, ale šlo jen o jednorázové šíření a 15,85 % šířilo dezinformaci již několikrát.



Graf 14 Šíření dezinformací

34) Důvěřuješ informacím, které sdílí tví oblíbení YouTubeři/influenceri/streameri?

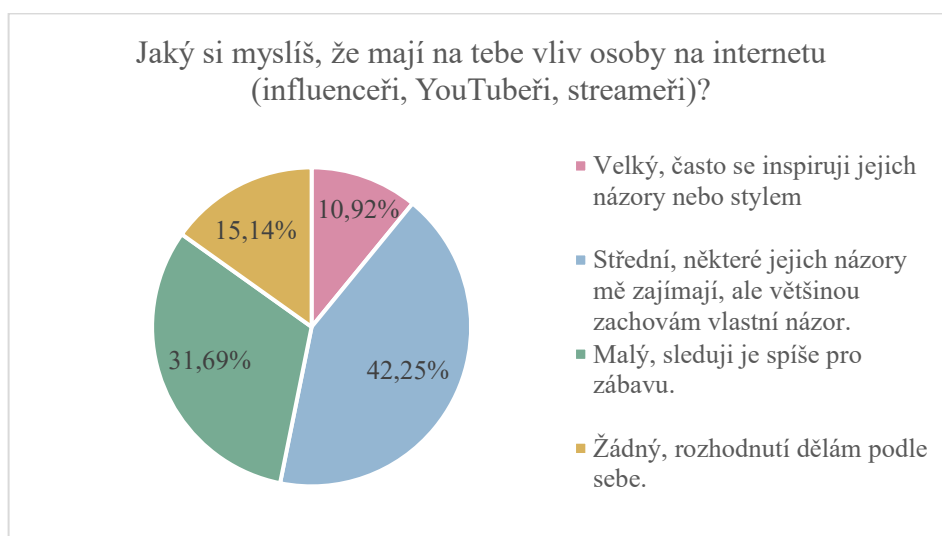
Třicátá čtvrtá položka se ptá na důvěru v osoby vystupující na sociálních sítích (viz 2.6). Jak vyplývá z následujícího grafického znázornění (Graf 15), 21,48 % sleduje tyto osoby spíše pro pobavení než jako zdroj validních informací. 34,15 % říká, že přemýšlí o sdíleném obsahu a snaží se informace ověřovat. Podle tématu se v důvěře rozhoduje 40,85 % pubescentů a maximální důvěru v tyto osoby má pouze 3,52 % dotazovaných.



Graf 15 Důvěra v osoby na sociálních sítích

35) Jaký si myslíš, že mají na tebe vliv osoby na internetu (influenceři, YouTubeři, streameři)?

V třicáté páté položce byli pubescenti dotazováni na vliv osob zmíněných v předešlé položce na ně samotné (Graf 16). Nejvíce dotazovaných, 42,25 %, většinou zachovává vlastní názor, ale některými názory se nechá ovlivnit. Za účelem pobavení je sleduje 31,69 % a zcela podle sebe se rozhoduje 15,14 % pubescentů. Nejméně, konkrétně 10,92 % z nich, tento vliv vnímá jako velký a jejich názory a stylem se často inspiroují.



Graf 16 Vliv osob vystupujících na internetu

36) Jaká rizika podle tebe mohou být spojena s tím, že lidé sledují tyto osoby?

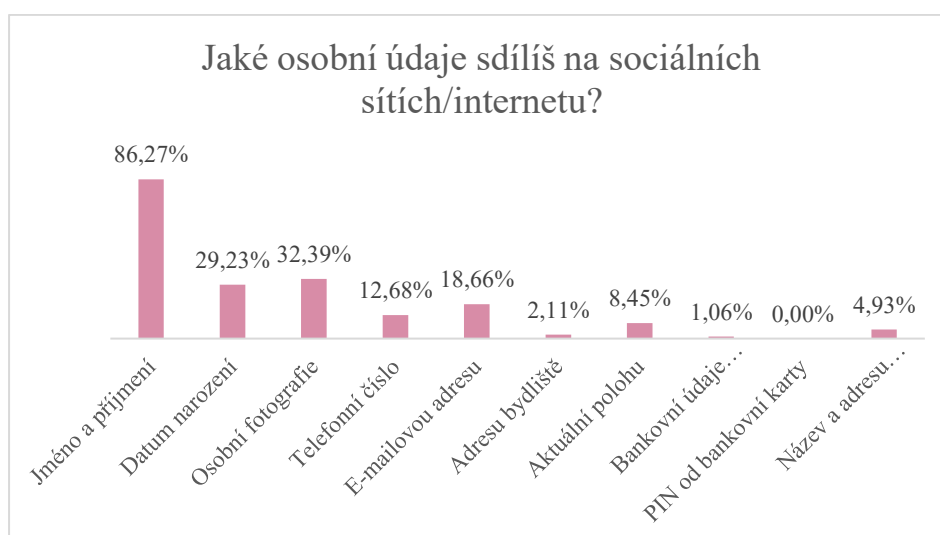
Třicátá šestá položka zjišťovala povědomí o rizicích spojených se sledováním osob zmíněné v předešlé položce z pohledu pubescentů. Analýza grafu uvedeného níže (Graf 17) ukazuje, že 41,55 % dotazovaných považuje za riziko ztrátu volného času nebo soustředění na jiné, důležitější věci jako je třeba rodina, škola a jiné. O něco méně pubescentů, konkrétně 35,56 %, uvádělo za rizikové sdílení nepravdivých nebo zavádějících informací, které mohou ovlivnit jejich rozhodování. Přílišnou idealizaci životního stylu vedoucí k nespokojenosti sebe samého vnímá 33,10 % pubescentů. Dále 29,93 % dotazovaných, kteří uváděli nátlak na nákup produktů nebo služeb, které nemusí být vždy kvalitní a potřebné v jejich životech. 23,59 %, tam nevidí riziko žádné.



Graf 17 Rizika spojená se sledováním osob vystupujících na internetu

37) Jaké osobní údaje sdílíš na sociálních sítích/internetu?

Třicátá sedmá položka se ptala na sdílení osobních údajů na internetu nebo konkrétněji na sociálních sítích (Graf 18). Většina pubescentů, konkrétně 86,27 % z nich, zveřejňuje své jméno a příjmení, 32,39 % svou osobní fotografii, a 29,23 % svůj datum narození. 18,66 % pubescentů sdílí svou e-mailovou adresu, své telefonní číslo 12,68 % a aktuální polohu 8,45 % dotazovaných. O něco méně, 4,93 %, adresu a název navštěvované školy, pouze 1,06 % bankovní údaje a nikdo PIN od bankovní karty.

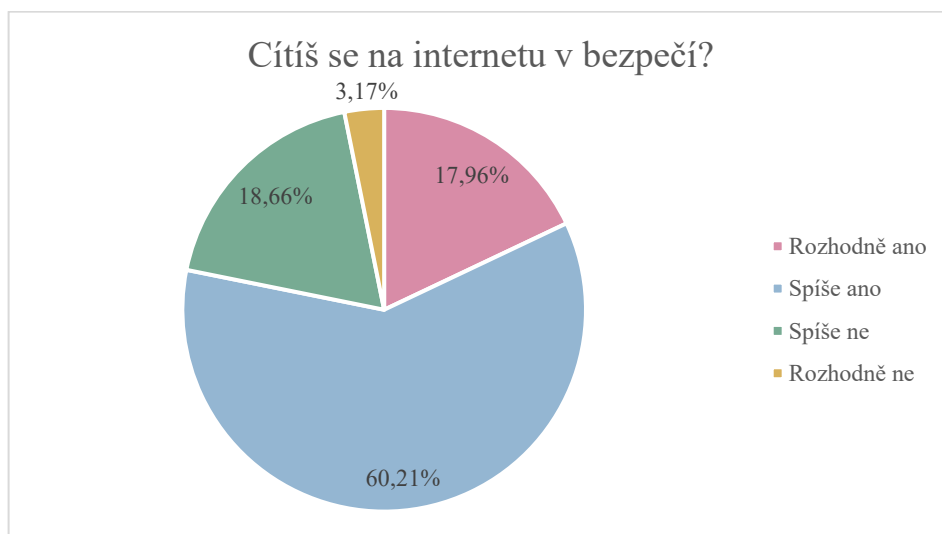


Graf 18 Sdílení osobních údajů na internetu

5.3 Jaké jsou pocity pubescentů při setkání s těmito riziky?

6) Cítíš se na internetu v bezpečí?

Šestá položka se týká pocitu bezpečí pubescenta při pohybu na internetu. Na výběr měli možnosti od rozhodně ano až po rozhodně ne. Dle grafu níže (Graf 19) lze říci, že se 60,21 % pubescentů na internetu cítí spíše bezpečně. 18,66 % pubescentů se zcela bezpečně necítí a o trochu méně, konkrétně 17,96 %, se naopak cítí v naprostém bezpečí. Nejméně pubescentů, konkrétně 3,17 % z nich, se cítí v naprostém nebezpečí.

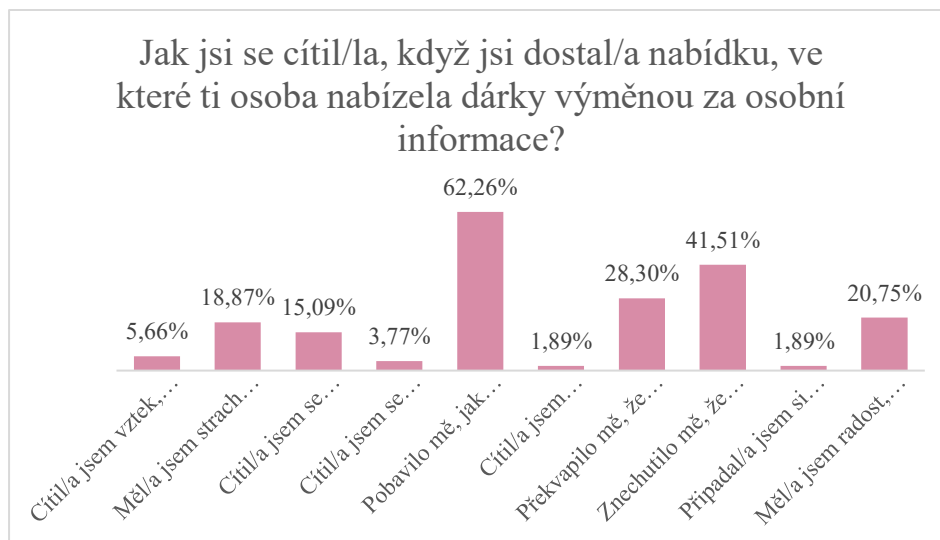


Graf 19 Pocit bezpečí

15) Jak jsi se cítil/la, když jsi dostal/a nabídku, ve které ti osoba nabízela dárky výměnou za osobní informace?

Patnáctá položka navazuje na předchozí a ptá se na pocity při zážitku rizika luringu (Graf 20). Bude počítáno s 53 pubescenty s tímto zážitkem. Nejvíce převažovala emoce radost, přičemž „pobavenost“ je dílčí emocí, a konkrétně šlo o pobavení, že na ně někdo zkouší takové triky a vybralo si ji 62,26 % pubescentů. Dále 41,51 % cítilo tzv. rozhořčený odpor, dílčí emoce znechucení, a to z důvodu zneužití důvěry v druhé. Překvapených z takové nabídky bylo 28,30 %, což spadá pod emoci překvapení. Další odpověď opět obsahuje emoci radost, přičemž je v jiném znění – „měl/a jsem radost, že jsem se nenechal/a nachytat,“ a odpovědělo na ni 20,75 % z dotazovaných. Strach nebezpečí pocíťovalo 18,87 % pubescentů a lze to zařadit od stejnojmennou emoci. Dílčí emoce strachu je nervozita, kterou cítilo dalších 15,09 % dotazovaných. Z důvodu neuvědomělosti, že jde o podvod cítilo 5,66 % vztek. Ten lze zařadit pod emoci hněvu a dílčí emoci rozhořčení. Pouhých 3,77 % pubescentů se cítilo zoufale, protože nevěděli, jak se zachovat v dané

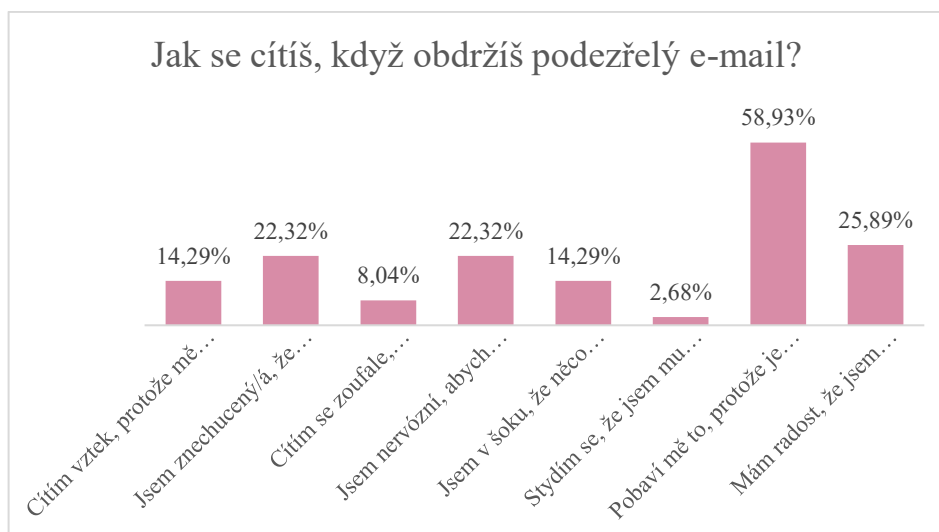
situaci, což patří pod emoci smutek a dílčí emoci zoufalství. Důvěru cítilo 1,89 % dotazovaných z důvodu toho, že věřili dané situaci, což patří pod emoci láska. Dalších 1,89 % se cítilo provinile, jelikož tomu na chvíli uvěřili, což je emoce hanba s dílčí emoci stud či vina. Jeden pubescent také nad rámec těchto odpovědí uvedl: „vůbec mě to nezajímalo, nezaujalo a ignoroval jsem to.“



Graf 20 Pocity u luringu

17) Jak se cítíš, když obdržíš podezřelý e-mail?

Sedmnáctá položka navazuje na šestnáctou a zaměřuje se na pocity při setkání s phishingem, počet pubescentů s tímto zážitkem je 112. Z níže uvedeného grafu (Graf 21) vyplývá, že nejvíce převládalo pobavení z dané situace, a to konkrétně 58,93 %. Pobavení lze zařadit pod emoci radost. Pod tuto emoci lze zařadit i další odpověď, která má ale jiné znění, a to „Mám radost, že jsem podezřelý e-mail poznal/a a nepodlehl/a tomu,“ kterou si vybralo 25,89 % pubescentů. Znechuceně se cítilo 22,32 %, přičemž tento pocit lze zařadit pod emoci rozhořčený odpor. Nervózně kvůli šanci nechtěného kliknutí na nebezpečný odkaz se cítilo opět 22,32 %. Vztek, který je součástí emoce hněvu a dílčí emoce rozhořčení, pociťovalo 14,29 %. V šoku z této situace bylo také 14,29 %, přičemž se řadí pod emoci překvapení. 8,04 % pubescentů se cítilo zoufale, jelikož nevěděli, jak se správně zachovat, přičemž zoufalství patří pod emoci smutku. Nejméně dotazovaných cítilo stud z chvilkové důvěry, a to konkrétně 2,68 %, kdy stud patří pod emoci hanba. Mimo tyto odpovědi dva pubescenti také uvedli: „Bylo mi to jedno“ a „Je mi to jedno, posílám to do bloku,“ což lze považovat za neutrální emoci. Pojem „blok“ znamená blokaci, v tomto případě zřejmě myšleno jako přesunutí e-mailu do kategorie spamu.



Graf 21 Pocity při setkání s phishingem

20) Jak jsi se cítil/a, když jsi zjistil/a, že máš v počítači malware? (např. virus, trojský kůň, adware atd.)

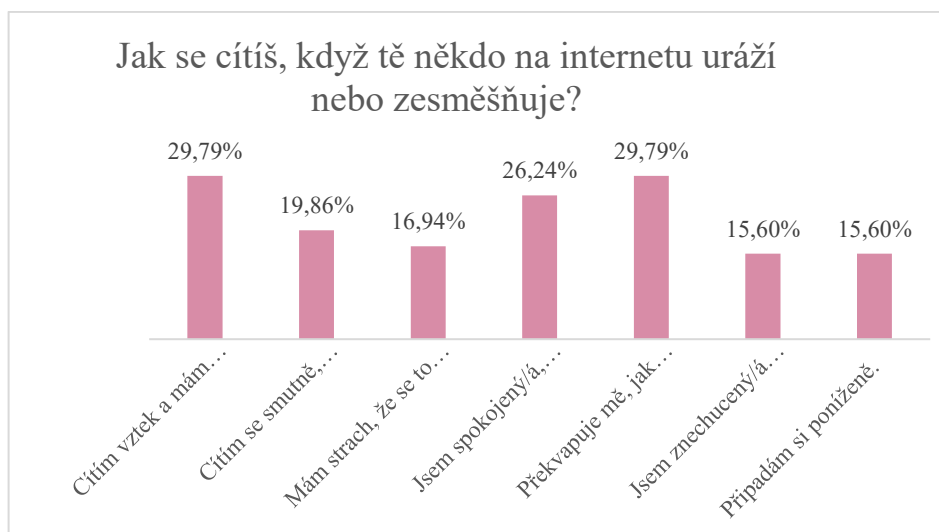
Dvacátá položka se dotazuje se na pocity pubescentů, když zjistili, že mají ve svém počítači nějaký malware, bude tedy pracováno s 67 pubescenty (Graf 22). Nejvíce, tedy u 44,78 %, se vyskytovala emoce hněvu a konkrétně pocit rozhořčení či zuřivosti. Emoci strach zažívalo 38,81 %, a to ze ztráty svých souborů na počítači. V šoku bylo 34,33 % pubescentů, přičemž to spadá pod emoci překvapení. 17,91 % se cítí trapně, že si na toto riziko nedali pozor, což je emoce hanba a dílčí emocí stud. Znechucení z malwaru v jejich počítači pociťovalo 13,43 %. Jedná se o emoci rozhořčeného odporu s dílčí emocí znechucení. 11,94 % bylo zklamaných, že se stali obětí, to je řazeno opět pod emoci hanba, ale dílčí emocí zklamání.



Graf 22 Pocit při stažení malwaru

25) Jak se cítíš, když tě někdo na internetu uráží nebo zesměšňuje?

Dvacátá pátá položka je zaměřena na pocity při urážení nebo zesměšňování jinými uživateli na internetu (Graf 23). Na úvod je potřeba říci, že tato položka nenavazuje na položku č. 22, jelikož byla zamýšlena na zesměšňování a urážení obecně, tzn. nejen skrze komentáře. Pokud by nebylo počítáno s těmi, kteří uvedli, že nenavštěvují sociální sítě (opět 3,52 %) nebo že nebyli nikdy zesměšňováni či uráženi (těch tedy bylo 143 neboli 50,35 %), tak by se počítalo s 141 pubescenty. 29,79 % z nich tedy uvedlo, že cítí vztek a má chuť útočnickovi něco vrátit zpět, to lze přiřadit k emoci hněv a dílčí emoci rozhořčení. Se stejným procentem také emoce překvapení, jak daleko jsou lidé schopni zajít. Dále emoce radost, dílčí emoce spokojenost, kde 26,24 % pubescentů uvádí, že se cítí spokojeně, když dokáží na urážky nereagovat. 19,86 % se cítí smutně a zasáhne je to, což spadá pod emoci smutku. Dále 15,60 % se cítí znechuceně ze zlostného chování lidí, přičemž to patří k emoci rozhořčeného odporu a dílčí emoci znechucení. Stejný podíl dotazovaných se cítí poníženě, což je emoce hanby a dílčí emoce poníženosti. 14,89 % má strach z opakování či eskalace útoku, tedy stejnojmenná emoce. Mimo tyto odpovědi celkem osm pubescentů uvedlo „Je mi to jedno,“ což lze považovat za neutrální emoci. Dále by sem bylo možné přiřadit další tři odpovědi, kde pubescenti uvedli, že to neřeší, nijak nereagují, protože je neznají, anebo že „prostě odpoví ok a pokračují svým dnem.“ Jeden pubescent uvedl, že „miluje ragebaitovat,“ kde zjednodušeně jde o úmyslné vyvolání vzteku, na podobném způsobu funguje flambait (viz 2.1.1). Další dva tvrdí, že útočníka začnou urážet také nebo s ním argumentují. Dva další to pobaví a vysmějí se mu, což lze přiřadit k emoci radosti s dílčí emocí pobavenosti. Poněkud alarmující odpověď by mohla být „zbiju ho venku,“ což by mohlo vést k závažnějším činům, jako je šikana a použití násilí ve formě odplaty. Poslední odpověď zde bude uvedena v celém znění: „Spíše, když se něco podobného stane, tak většinou ti lidi, co mě/někoho zesměšňují mají účet, na kterém je nikdo nesleduje. Jde vidět, že ti lidi se bojí, kdyby je někdo poznal a takové lidi, co se skrývají neberu vážně.“

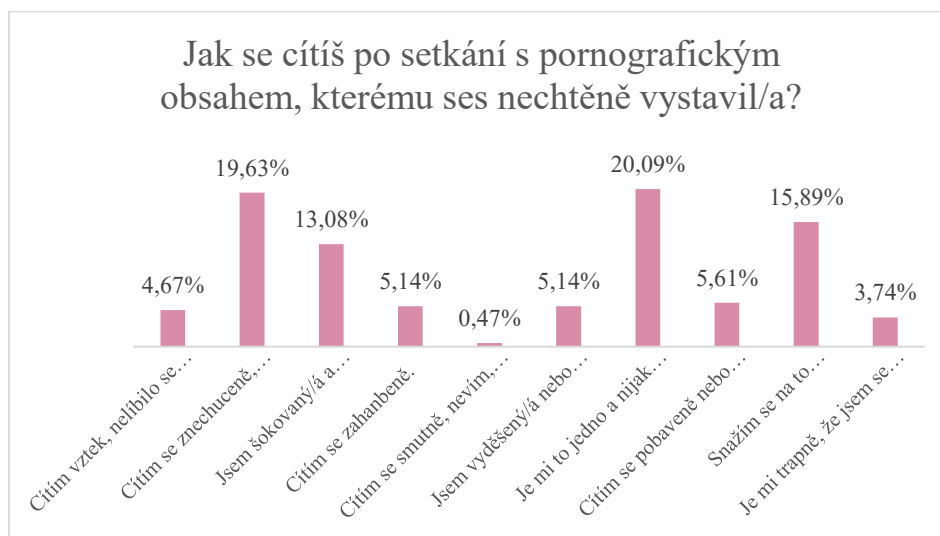


Graf 23 Vlastní pocity při zesměšnění či urážení

27) Jak se cítíš po setkání s pornografickým obsahem, kterému ses nechtěně vystavil/a?

Dvacátá sedmá položka navazuje na předchozí položku a ptá se pubescentů na pocity při setkání s pornografickým materiálem, kterému byli nechtěně vystaveni (Graf 24). Z těch, kteří do této situace dostali (124), zastává 34,68 % neutrální pocity, respektive je to nijak neovlivnilo a nezáleží jim na tom. O něco méně dotazovaných, 33,87 %, se cítí znechuceně, což v typologii emocí patří pod rozhořčený odpor, dílčí pak znechucení. K další neutrální reakci patří 27,42 % pubescentů, která byla akorát jinak formulovaná: „Snažím se na to zapomenout a ignorovat to.“ Dále 22,58 % je při setkání šokovaných a překvapených, že se s tím vůbec setkali, to je zařazeno pod emoci překvapení a dílčí emoci šok. 9,68 % pubescentů se cítí pobaveně a zvědavě, i přestože vědí, že by to neměli vidět. Tuto odpověď lze zařadit pod emoci radosti s dílčí emoci pobavenosti. 8,87 % se cítí zahanbeně neboli emoce hanby, a stejný podíl se cítí vyděšeně nebo nervózně, tedy emoce strachu, dílčí je pak nervozita a děs. Dále 8,06 % cítí vztek, že jim nevhodný obsah někdo poslal, to znamená emoci hněvu a dílčí emoci rozhořčení. Pouhých 6,45 % se cítí trapně, že se do této situace vůbec dostali, přestože nechtěli, což je opět zařazeno pod emoci hanba s dílčí emoci stud, s rozdílem jiné formulace odpovědi. Pouze jeden pubescent (0,81 %) uvedl, že se cítí smutně, přičemž neví, jak danou věc zpracovat. To lze zařadit pod emoci smutku. Kromě těchto odpovědí 0,81 % pubescentů uvedlo, že se jim to nelíbí a nahlásí to, tedy rozhořčený odpor, dílčí emoce nelibosti, dále že to byl tzv. bot. Ten lze popsat jako automatický program, který rozesílá nahé fotky na sociální síti Instagram, často za účelem spamu či podvodu. Poslední odpověď se týkala toho, že pubescentovy pocity záleží i na tom, kdo zprávy či fotografie zasílá, například pokud je zasílatelkou vrstevnice, necítí příjemce tolik

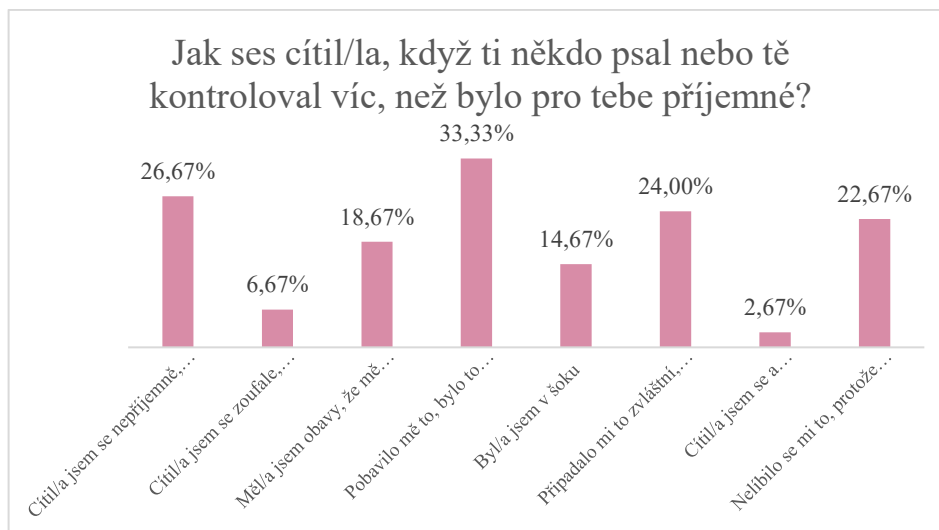
negativních emocí, ale v případě, kdy nevhodný materiál zasílá dospělý muž, je možné hovořit o formě obtěžování.



Graf 24 Pocity při setkání s pornografickým obsahem

30) Jak ses cítil/la, když ti někdo psal nebo tě kontroloval víc, než bylo pro tebe příjemné?

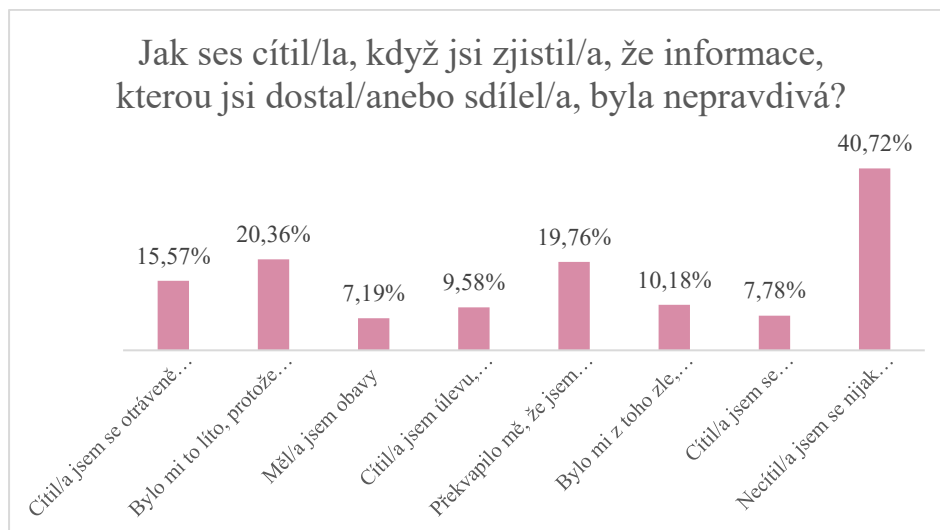
Třicátá položka dále zjišťovala pocity po setkání s nadměrným zájmem, na který byli pubescenti dotazováni v předešlé položce. Bude zde proto počítáno se 75 dotazovanými, kteří se s tímto jevem setkali (Graf 25). Nejvíce se vyskytovala emoce radosti (dílčí emoce pobavenosti), přičemž 33,33 % se cítilo pobaveně. Naštvaně se cítilo 26,67 %, což spadá pod emoci hněvu s dílčí emocí podrážděnost, rozhořčení či popuzenosti. Neutrální pocit zastávalo 24 % pubescentů, rozhořčený odpor (dílčí emoce nelibosti) dále 22,67 % a strach (dílčí emoce obavy) ze sledování mělo 18,67 % dotazovaných. Mezi menší podíl patří 6,67 %, kteří se cítili zoufale a nevěděli, jak se v dané situaci zachovat, což se řadí do emoce smutku. Nejméně pubescentů, 2,67 %, se cítilo trapně, jelikož neustále zaznamenávali pocit zasahování do svého soukromí. Kromě již předepsaných odpovědí dva dotazovaní také uvedli, že jim to bylo jedno a ignorovali daný jev a jeden si dokonce uživatele zablokoval.



Graf 25 Pocity při nadměrném zájmu jiným uživatelem

32) Jak ses cítil/la, když jsi zjistil/a, že informace, kterou jsi dostal/anebo sdílel/a, byla nepravdivá?

Tricátá druhá položka se dále zaměřuje na pocity při setkáním s dezinformací. Bude zde počítáno se 167 pubescenty, kteří v předešlé otázce uvedli, že se s tímto jevem setkali. Graf níže (Graf 26) ukazuje, že neutrální pocit mělo 40,72 % dotazovaných, přičemž to nijak zvlášť nevnímali. Dále 20,36 % pocíťovalo hanbu (dílčí emoce lítosti), protože uvěřili dané informaci. O něco méně dotazovaných, konkrétně 19,76 %, bylo překvapených, že se nechali tak snadno oklamat (emoce překvapení). Vztek nebo otrávení cítilo 15,57 %, to je řazeno pod emoci hněv s dílčí emocí rozhořčení a otrávenost. Znechuceně se cítilo 10,18 %, jelikož měli pocit manipulace. Tento pocit lze zařadit pod emoci rozhořčeného odporu, dílčí emoce pak znechucení. Úlevu ve smyslu toho, že se jim nic nestalo a akorát si z toho vzali ponaučení, pocíťovalo 9,58 % pubescentů. Lze tedy říci, že pocíťují radost, kde dílčí emocí této emoce je právě úleva. 7,78 % dotazovaných se cítilo poníženě, jelikož uvěřili něčemu nepravdivému, což patří k emoci hanba a dílčí emoci ponížení. Nejméně pubescentů, tedy 7,19 %, mělo obavy, které lze řadit pod emoci strachu (dílčí emoce obavy). Nad rámec těchto odpovědí také jeden dotazovaný tvrdí, že jej to rozesmálo. Pobavenost je dílčí emocí radosti. Dva další uvedli, že jim to bylo jedno, to lze řadit pod neutrální emoce. A v poslední odpovědi: „nevadilo mi to, aspoň vím, že si mám informace ověřovat,“ lze říci, že si pubescent vzal ponaučení do budoucna.



Graf 26 Pocity při setkání s dezinformací

5.4 Jaké strategie užívají pubescenti v prevenci rizik spojených s používáním digitálních technologií?

38) Jak reaguješ, když dostaneš zprávu od neznámého člověka na sociálních sítích?

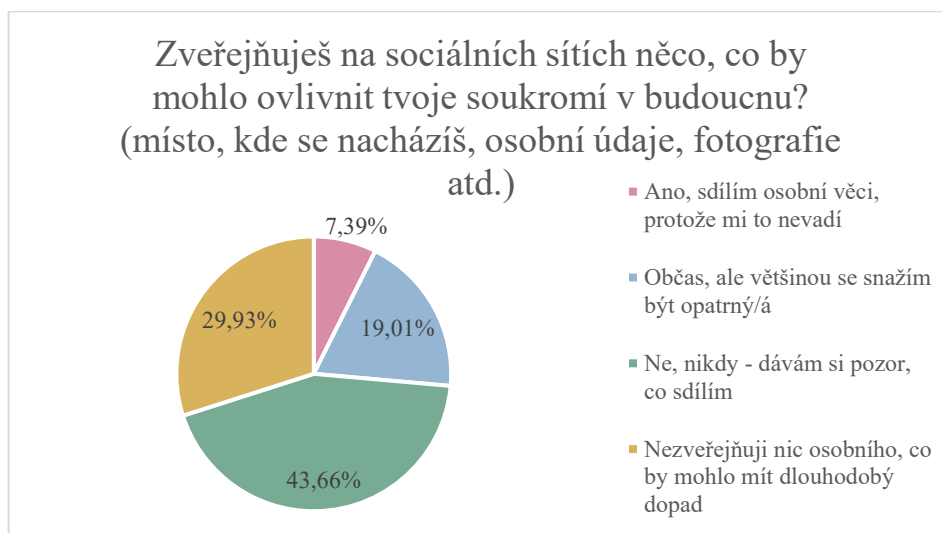
Dále třicátá osmá položka, která se dotazovala na to, jakým způsobem pubescenti reagují na zprávy od neznámé osoby na sociálních sítích (Graf 27). 25,35 % dotazovaných cizí osobu ignoruje. Odpoví 21,48 % pubescentů, přičemž ale opatrně. Se zájmem, pokud je ovšem zpráva zdvořilá a zajímavá, odpoví 19,72 %. O něco méně, konkrétně 17,96 %, účet ihned zablokuje a 15,49 % nikdy cizí zprávu ani nedostalo.



Graf 27 Reakce na zprávu od cizí osoby

39) Zveřejňuješ na sociálních sítích něco, co by mohlo ovlivnit tvoje soukromí v budoucnu? (místo, kde se nacházíš, osobní údaje, fotografie atd.)

Třicátá devátá položka se zaměřuje na zveřejňování informací na internetu, které by mohly mít dopad na soukromí v budoucnu (Graf 28). Nejvíce, tedy 43,66 % pubescentů, zastávalo takového názoru, že si dává pozor na sdílený obsah a nikdy nesdílí nic takového. Nic osobního s dlouhodobým dopadem nezveřejňuje 29,93 % dotazovaných, lze sem řadit např. kontroverzní názory na různá témata nebo informace, které neobsahují citlivé nebo osobní údaje, jako jsou fotky jídla, dovolené (i bez přesné lokace) a další. 19,01 % připouští, že občas zveřejní něco, co by mohlo v budoucnu ovlivnit jejich soukromí, ale většinou se snaží zachovat opatrnost. Nakonec 7,39 % pubescentů, kteří tyto informace sdílí, protože jim to nevadí.



Graf 28 Zveřejňování informací s rizikem ovlivnění do budoucna

40) Přijímáš žádosti o přátelství nebo sledování od lidí, které osobně neznáš?

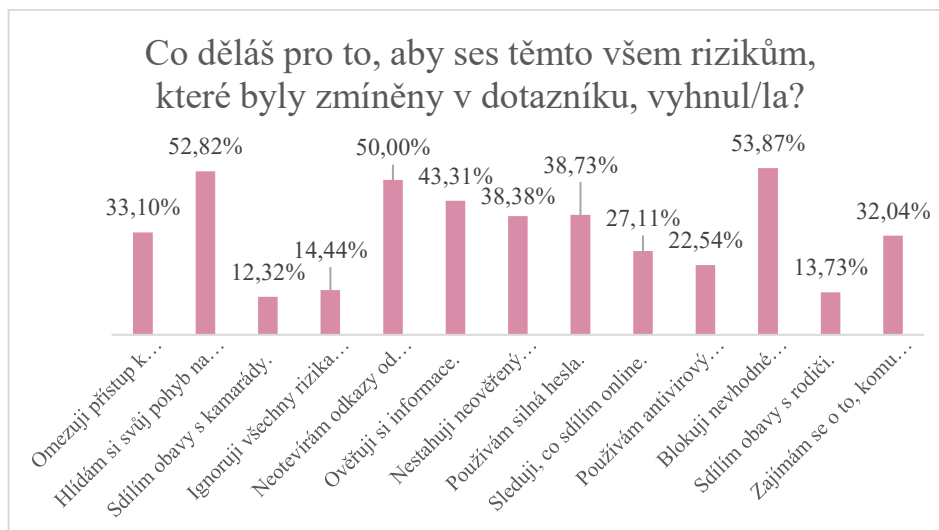
Čtyřicátá položka se ptá svým způsobem na prevenci vůči setkání s potenciálními riziky (Graf 29). Téměř polovina, konkrétně 42,96 % pubescentů, tvrdí, že nikdy žádosti o přátelství či sledování cizími lidmi nepřijímají. Pod podmínkou společných přátel žádost potvrdí 35,92 % dotazovaných, může se tedy jednat o zcela cizí osobu, ale mezi svými přáteli či sledovanými má přítele pubescenta. Žádost či sledování cizí osobou vždy potvrdí 17,61 % dotazovaných a opět je zde stejných 3,52 %, kteří sociální síť nemá.



Graf 29 Žádost o přátelství nebo sledování cizími lidmi

41) Co děláš pro to, aby ses těmto všem rizikům, která byly zmíněny v dotazníku, vyhnul/la?

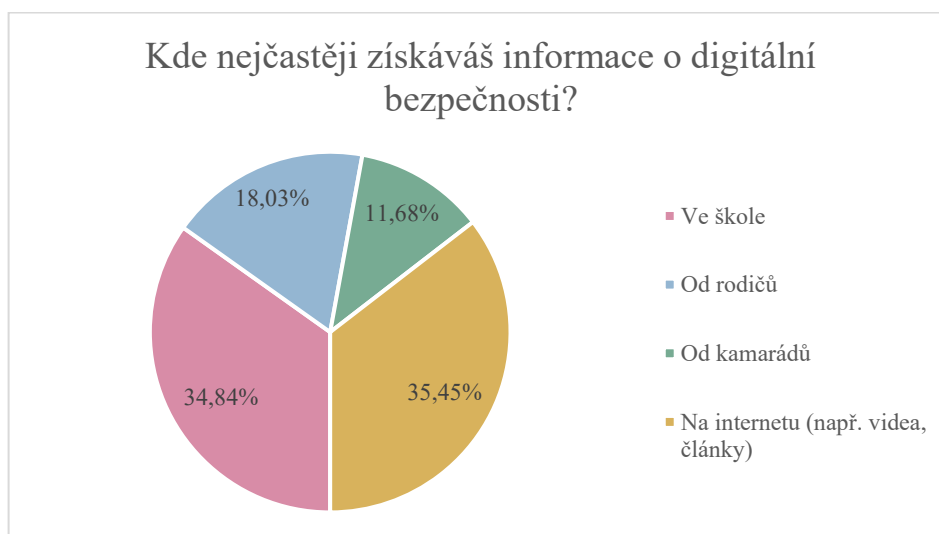
Čtyřicátá první položka je zaměřena pohled pubescentů na udržení jejich vlastní bezpečnosti při pohybu na internetu (Graf 30). Nejvíce, 53,87 %, uvedlo, že blokuje nevhodné uživatele. Dále 52,82 % tvrdí, že si svůj pohyb hlídá. Lze si představit zvýšenou pozornost při vstupu na různé webové stránky, zodpovědnost, kontrolu času na internetu, opatrnost a další. Přesná polovina, 50 %, k podpoře své bezpečnosti neotevívá odkazy od cizích osob. Informace si ověřuje 43,31 % dotazovaných a 38,73 % tvrdí, že používá silná hesla. Dále 38,38 % nestahuje neověřený obsah, který by mohl obsahovat nějaký druh malwaru (viz 2.2.2). Přístup na některé weby nebo aplikace nějakým způsobem omezuje 33,10 % pubescentů. O to, komu jaké informace sdělují, se zajímá 32,04 %. Pozor na to sdílený obsah si dává 27,11 % a pouhých 22,54 % uvádí, že používá antivirový program. Zde lze z části předpokládat, že pubescenti spoléhají na Windows defender (viz 4.2) a nestahují jiné antivirové programy. Veškerá rizika ignoruje 14,44 %, to znamená, že se tolik nezabývají online bezpečností a nezabývají se možnými riziky (tzn. sdílení citlivého obsahu, neověřování informací atd.). S rodiči sdílí obavy pouze 13,73 % pubescentů a s kamarády ještě méně, a to 12,32 %.



Graf 30 Prevence z pohledu pubescentů

42) Kde nejčastěji získáváš informace o digitální bezpečnosti?

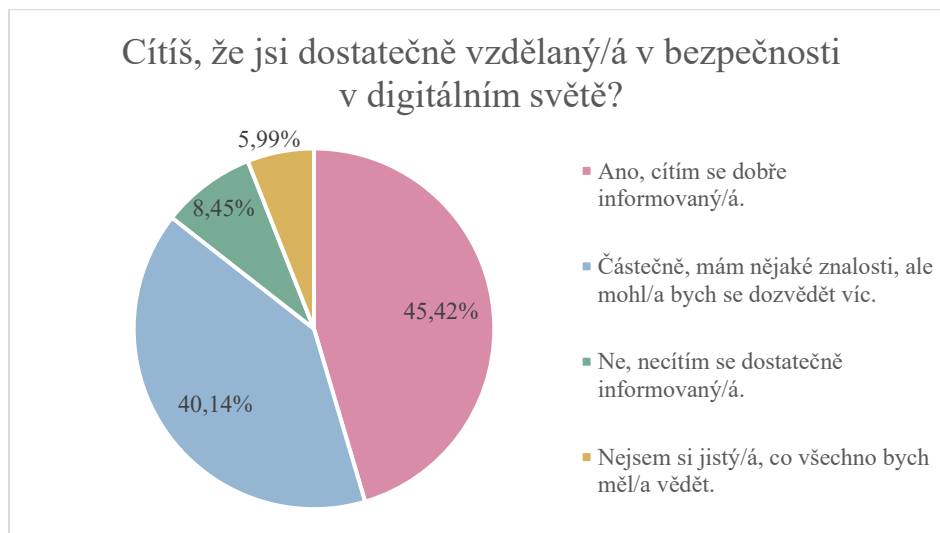
Čtyřicátá druhá položka se také týká prevence a konkrétně odkud pubescenti získávají informace o bezpečnosti v digitálním prostředí (Graf 31). Nejčastějším zdrojem je pro pubescenty internet, respektive různé články či videa, a týká se to 60,92 %. O něco méně (59,86 %) získává informace ve škole. Od rodičů 30,99 % a nejméně od svých kamarádů, a to 20,07 %. Dotazovaní mimo to uváděli odpovědi do kolonky „Jiné“. Dva z pubescentů uvedli sourozence, z čehož jeden konkrétně uvedl sestru. Dále jeden pubescent využívá jako zdroj informací televizi. Poslední odpověď: „Měli by dávat přednášky o bezpečnosti na internetu už od 1. třídy kvůli tomu, že mnoho dětí je nekontrolovaně na internetu,“ u které lze sledovat zajímavý a uvědomělý pohled pubescenta na dnešní dobu a bezpečnost.



Graf 31 Zdroj informací o digitální bezpečnosti

43) Cítíš, že jsi dostatečně vzdělaný/á v bezpečnosti v digitálním světě?

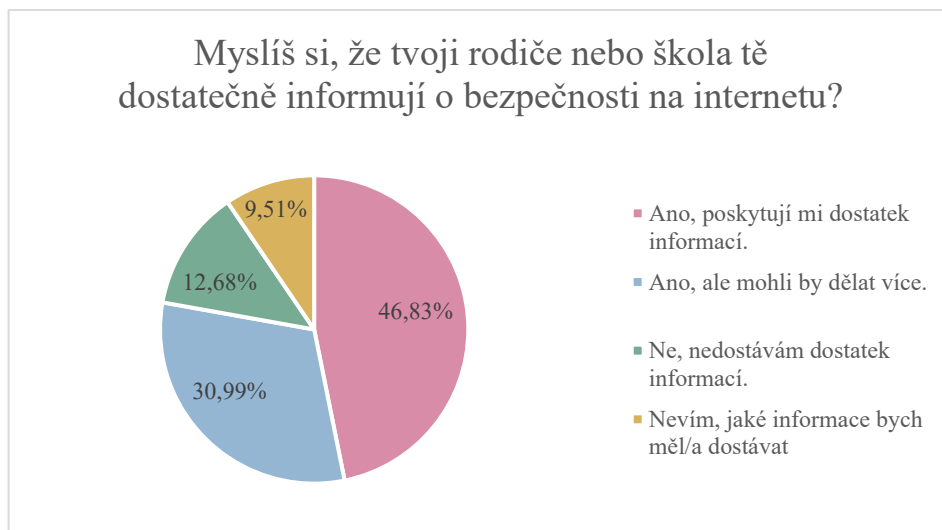
Dále čtyřicátá třetí položka, která je zaměřena na pocit vzdělanosti z pohledu pubescentů. Z uvedeného níže grafu (Graf 32) vyplývá, že 45,42 % dotazovaných se cítí dobře informovaní v oblasti bezpečnosti. Více by se chtělo dozvědět 40,14 %, i přesto, že něco málo ví. Nedostatečně vzdělaně se cítí pouhých 8,45 % a 5,99 % si není jistých, co všechno by o této problematice měli vědět.



Graf 32 Pocit vzdělanosti o bezpečnosti v digitálním světě

44) Myslíš si, že tvoji rodiče nebo škola tě dostatečně informují o bezpečnosti na internetu?

Poslední položka se dotazuje, jak pubescenti vnímají informovanost ze strany školy nebo rodičů (Graf 33). Nejvíce pubescentů, konkrétně 46,83 %, tvrdí, že jim poskytují dostatek informací. Větší příjem informací ze strany rodičů či školy vyžaduje 30,99 % dotazovaných. 12,68 % uvedlo, že nedostávají dostatek informací a 9,51 % neví, jaké informace by měli od rodičů nebo školy dostávat.



Graf 33 Vnímání informovanosti o bezpečnosti ze strany rodičů či školy

6 SHRNUTÍ VÝSLEDKŮ A INTERPRETACE DAT

V této kapitole bude shrnuta analýza výsledků a zároveň budou zodpovězeny výzkumné otázky. Nejprve bude zodpovězena a rozvedena první dílčí otázka, která se dotazuje na znalost rizik a odkud se o nich dozvěděli. Další část se zaměří na zodpovězení těch zbylých, přičemž bude ukázána provázanost a souvislost mezi odpověďmi napříč dílčími otázkami.

Na základě provedené analýzy dat byla identifikována tři nejznámější rizika, mezi kterými pubescenti uvádí **kyberšikanu, sexting a kybergrooming**. Hlavním zdrojem informací o rizicích je právě **internet** a následně škola. Rodiče jsou až na čtvrtém místě (z pěti), což potvrdilo teorii o odporu pubescentů k autoritám a snaze neodhalit příliš mnoho ze svého soukromí k předejití konfliktům s rodiči, popsanou v první kapitole. I přes větší informovanost školy či rodičů pubescenti volí jako hlavní zdroj internet, který by mohl být vnímán jako rizikové prostředí, z důvodu existence dezinformací a online agresorů.

Stejně jako zmiňují autoři Smahel et al. (2020), tak byl potvrzen nebezpečný výskyt rizik, se kterými se pubescenti setkávají. Lze říci, že i přestože se většina pubescentů cítí na internetu v bezpečí, a komunikaci s neznámým člověkem vnímá jako nebezpečnou, většinově k této komunikaci dochází. Tato zjištění překračují výsledky výzkumu od Szotkowski et al. (2013), kteří uvádí něco málo nad polovinu adolescentů, to samé také od autorky Hykyšové (2019). Takové chování může přispět k pravděpodobnosti setkání s riziky jako například kybergrooming. S jeho formami se setkala přibližně jedna třetina, přičemž na **osobní schůzku s cizím člověkem** dorazí každý desátý pubescent, což je rozdíl oproti výzkumům od autorů Szotkowski et al. (2013) i autorky Hykyšové (2019), kteří uvádí polovinu. To lze vysvětlit změnou trendů a zvyklostí co se týče seznamování online, například po období pandemie onemocnění covid-19, kdy se lidé museli spoléhat jen na online komunikaci. Zhruba každý pátý pubescent dostal **nabídku výměny osobních či citlivých informací za dárek**, přičemž valná většina projevila svou uvědomělost a na tuto techniku rizika kybergrooming nepřistoupila. Na druhou stranu ale dva pubescenti ano, jeden pod nátlakem a druhý dobrovolně. I přes vážnost rizika to většinu pubescentů **pobavilo**, což naznačuje vnímání rizika jako nezajímavé či neškodné, to lze vnímat jako alarmující. Další reakce zahrnovaly pocit **znechucení** ze zneužití důvěry a **překvapení**.

Mezi tři nejpoužívanější místa komunikace s cizím člověkem patří **hraní her a sociální sítě Instagram a Tik Tok**. Za alarmující lze pokládat zjištění o platformě **WhatsApp**, která je, stejně jako zmíněné sociální sítě, dostupná se souhlasem rodičů od 13

let (jinak od 15), ale také je k jejímu užívání potřeba telefonní číslo, které je následně dále dostupné ostatním uživatelům, kteří s ním mohou jakkoliv nakládat.

Možný projev **kyberstalkingu**, kdy šlo o pocit neustálé kontroly, popřípadě komentování příspěvků a projevu až příliš velkého zájmu druhým člověkem, zažil téměř každý čtvrtý pubescent. Nejvíce pubescentů to **pobavilo** a považovali to za přehnané, což by mohlo odrážet nedostatek povědomí o vážnosti jevu. Některými byl vnímán **neutrálně** a považován za zvláštní situaci, ale opět ji nevnímali jako ohrožující, což je zarážející. Riziko také velké části vyvolalo negativní emoce, kdy byly ze situace **naštvaní** nebo se jim zasahování do soukromí nelíbilo.

Přibližně každý druhý pubescent obdržel **podezřelý e-mail**, který mohl obsahovat odkaz s nebezpečným obsahem a každý třetí na něj klikl, přestože polovina v položce zaměřené na prevenci považuje neotevírání odkazů od cizích osob za svou formu prevence. Je zde viditelný rozpor mezi konkrétním zážitkem a tvrzením o svém bezpečném chování, které obecně velká většina považuje za bezpečné. Toto riziko je nejčastěji vnímáno s **pobavením** jako hloupost, respektive ho pubescenti vůbec neberou vážně. Na druhou stranu pocity zahrnovaly **radost** z nepodlehnutí podvodu, což ukazuje určitou míru obezřetnosti. Někteří byli **znechuceni** ze stálého výskytu nebo byli nervózní, aby odkaz omylem nerozklikli. Za pozitivní by tedy bylo možné považovat skutečnost, že si dospívající chtějí dát pozor. S nechtěným stažením **malwaru** se setkala téměř čtvrtina, což na předchozí riziko může, ale také nemusí navazovat, jelikož kromě možnosti stažení při phishing útoku existuje varianta při stahování z neověřených zdrojů. Tato situace je většinově vnímána negativně, což má své opodstatnění. Nejčastěji jsou pubescenti **naštvaní** nebo mají **strach** ze ztráty svých souborů, což odráží obavu o své soukromí. Pro některé byl zážitek **překvapivý** a mohl způsobit vysokou úroveň stresu.

Ačkoliv téměř polovina respondentů uvádí, že si informace ověřuje, výsledky ukázaly příjem **dezinformací** u každého druhého pubescenta, přičemž každý třetí ji někdy sdílel dál. To může naznačit nedůslednost při ověřování, případně že není prováděno dostatečně v žádoucích situacích. Když dostali dezinformační zprávu, většinově k ní zaujali **neutrální postoj** a nevnímali ji jako závažnou. To by mohlo vést k rychlému šíření a zvýšení rizika manipulace. Další zase vyjádřili **lítost**, že věřili nepravdivé informaci nebo byli **překvapení** ze snadného oklamání, což by ale mohlo vést k ponaučení do budoucna. Z výsledků také vyplynulo, že téměř polovina pubescentů byla někdy na internetu zesměšňována, ať už skrze komentáře nebo příspěvky apod. Dalo by se tedy říci, že byli

vystavení formě **kyberšikany**. Při setkání většina vyjádřila silné emoce, přičemž mnozí cítili **vztek** a touhu vrátit útok dané osobě zpět. Stejně tak byli **překvapení**, jak daleko jsou lidé schopni zajít. Na druhou stranu byli někteří **spokojení**, když se dokázali vzdát reakcí na urážky, a další zase pocíťovali **smutek**. I přesto, že má většina negativní postoj k urážení a zesměšňování na internetu, každý čtvrtý přiznal, že sám napsal **nenávistný nebo zesměšňující komentář** druhému člověku. To poukazuje na nesoulad mezi tím, když se stanou oběti sami a naproti tomu, když se tak chovají vůči ostatním. Stejně jako ve výzkumu Freeda et al. (2023) byl potvrzen výskyt nenávistných komentářů, přičemž se s nimi setká každý třetí pubescent pod svými příspěvky. Tato zjištění jsou v souladu s výzkumem od autorů Szotkowski et al. (2013). Pokud narazí na takové komentáře tak se je většina snaží ignorovat, jiným se to nelíbí nebo zůstanou v šoku z takového chování. Jen menšina je schopna se druhého zastat a podpořit ho, ale raději se nezapojí, aby se sami nestali terčem nenávisti.

Přibližně polovina obdržela **pornografický materiál**, ať šlo o fotky, nebo videa obsahující nahotu. Minimum přiznalo, že sami někdy poslali takový materiál, a to buď svůj vlastní nebo dříve sdílený někým jiným. Zjištění je ale v rozporu s výzkumem autorů Szotkowski et al. (2013), kteří uvádějí větší četnost výskytu. Dále každý pátý zná někoho, kdo tuto situaci zažil. Zde se lze jen domnívat, zda se nesnažili vyhnout přímé odpovědi a místo toho se skryli pod jinou odpověď. Pocity zaujímají spíše **neutrální**, přičemž tato lhostejnost by mohla naznačovat jejich odlišné vnímání takového obsahu oproti předchozí generaci, které se stalo do jisté míry běžnou součástí online prostředí, se kterou se naučili svým způsobem vyrovnávat. Velká část pubescentů však také vyjádřila odmítavý a **znechucený** postoj, což je pochopitelné, a také snahu tento zážitek potlačit a ignorovat. Někteří byli v **šoku** z této situace, což by mohlo svědčit o nezkušenosti s tímto obsahem a jeho nečekané zobrazení narušilo jejich pocit bezpečí.

Osoby na internetu mohou mít na pubescenty významný vliv, který většina vnímá spíše jako **inspirativní** a většinou si nechají svůj názor. Obecně jim ale **záleží na daném tématu** a na základě něj se pubescenti rozhodují, zda v dané oblasti osobám, sdílející informace, svěří svou důvěru, nebo ne, případně si informace ověřují. Jak bylo již zmíněno výše, pravda to ale, jak říkají, není. Nejvíce vnímají **ztrátu času** na důležitější činnosti. Také **sdílení nepravdivých informací**, které by mohlo ovlivnit jejich rozhodování. To lze vnímat pozitivně, je zde viditelná uvědomělost ohledně odvádění pozornosti a snižování produktivity. Vnímají ale také **přílišnou idealizaci životního stylu**, čímž se projevuje jejich

kritické myšlení a mohli by se tak soustředit na svou autentičnost, což přispěje zdravému vztahu k sobě samému.

Mezi nejčastěji sdílené osobní údaje pubescentů patří **jméno a příjmení, osobní fotografie a datum narození**, což se od výsledků výzkumu od autorů Szotkowski et al. (2013) odlišuje datem narození. Ve zmíněném výzkumu vyšla na prvních třech místech také e-mailová adresa. Pozitivním zjištěním je, že žádný pubescent neuvádí **PIN od své bankovní karty**, to ukazuje na zodpovědnost a opatrnost, jelikož by sdílení tohoto údaje mohlo vést k finančnímu podvodu nebo ke krádeži identity. Tato zjištění korespondují s jejich **opatrným postojem ke zveřejňování citlivých informací**, které by mohly ovlivnit jejich soukromí do budoucna.

Zatímco autoři Szotkowski et al. (2013) zmiňují výrazně menší výskyt, na základě výsledků tohoto výzkumu lze říci, že pubescenti vykazují různé přístupy k **žádostem o přátelství či sledování od lidí, které osobně neznají**. Polovina pubescentů si přidá cizího člověka mezi přátele, přičemž každý šestý si ho přidá bez váhání. To na jednu stranu ukazuje jejich otevřenost k novým kontaktům, na druhou stranu to ale nese i svá rizika. Většina si ale přidává jen ty osoby, které zná osobně. Na zprávy od cizích osob pubescenti nejčastěji nijak nereagují nebo odpoví s opatrností. Každý pátý ale na tuto zprávu odpoví, ale jen pokud je zdvořilá. Obecně uvádějí různé způsoby prevence vůči rizikům v online prostředí. Nejčastějším opatřením je **blokace nevhodných uživatelů, hlídání si pohybu online**. To znamená, že si dávají pozor, jaké stránky navštěvují a na co klikají, což naznačuje silný důraz na ochranu svého soukromí. Mnozí také tvrdí, že **neotevírají odkazy od cizích osoby** a že si ověřují informace. To však bylo vyvráceno při dotazování na reálné zkušenosti, kdy byla zjištěna jejich neopatrnost v těchto dvou směrech. Ke své ochraně také používají **silná hesla a nestahují neověřený obsah**, přitom ale téměř u čtvrtiny došlo ke stažení nějakého druhu malwaru. O **bezpečnosti na internetu** se ale paradoxně vzdělávají na **internetu**, a následně také ve **škole**.

Většina pubescentů se považuje za alespoň **částečně informované**, přičemž jejich zkušenosti ukazují opak. Na druhou stranu lze říci, že většina **požaduje větší míru informovanost** o bezpečnosti v digitálním světě, zároveň vyjadřují **požadavek na větší přísun informací o bezpečnosti ze strany školy nebo rodičů**. To naznačuje, že dospívající mají zájem o lepší vzdělávání a podporu v oblasti online bezpečnosti.

ZÁVĚR

Tato práce se zaměřila na pohled pubescentů na rizika v digitálním světě. V dnešní době jsou nedílnou součástí života téměř všech lidí, a to především mladší generace, digitální technologie. S jejich rychlým a neustálým vývojem se také vyvíjí rizika, která se v něm nachází. Tím je tato práce aktuální. Pubescenti tvoří zranitelnou skupinu z důvodu nedostatečných životních zkušeností, s čímž souvisí ne zcela dostatečně vyvinuté bezpečnostní strategie.

Lze říci, že došlo k naplnění všech výzkumných cílů a zodpovězení výzkumných otázek. Práce poskytuje komplexní pohled na problematiku digitální bezpečnosti a také na to, jak mladí lidé vnímají tyto hrozby a jaké strategie používají ke své obraně. Jejich pohled na své chování byl často v rozporu se zkušenostmi s konkrétními riziky, což naznačuje, že i přes vědomost rizik v digitálním světě a znalost bezpečnostních opatření, ne vždy tato opatření dodržují. Tato rizika jsou, i přes jejich vážnost, častokrát brána na lehkou váhu nebo s jistou dávkou pobavení, což může být způsobeno nedostačenou informovaností nebo přehnaným pocitem bezpečí. Většina mladých lidí čerpá informace o digitálních hrozbách a bezpečnosti z internetu, což však zároveň přináší riziko, jelikož samotný internet může být místem pro šíření nepravdivých a zavádějících informací a pubescenti je nemusí vždy rozpoznat.

Na závěr je potřeba zdůraznit prevenci, která hraje klíčovou roli v bezpečném pohybu v online prostředí. Ukazuje se zde význam potřeby zvýšené informovanosti, a to nejen mezi pubescenty, ale také v širším pohledu, včetně rodičů nebo škol. Důležitým zjištěním je, že i když pubescenti mají teoretické povědomí o rizicích, často setkávají se situacemi, které vyžadují i správný způsob aplikace nabytých vědomostí v praxi. Výsledky výzkumu mohou přispět k rozvoji metod prevence a vzdělávání v oblasti digitální bezpečnosti, které se zatím zdají být nedostatečně efektivní. Místo na varování před nebezpečím by se tyto metody prevence mohly zaměřit na podporu kritického myšlení v hodnocení informací, které dospívající čerpají z internetu. Základní myšlenkou by bylo naučit mladé uživatele internetu udržet informovanost a zodpovědný přístup k online světu.

SEZNAM POUŽITÉ LITERATURY

ČERNÁ, Alena; DĚDKOVÁ, Lenka; MACHÁČKOVÁ, Hana; ŠEVČÍKOVÁ, Anna a ŠMAHEL, David, 2013. *Kyberšikana: průvodce novým fenoménem*. Psyché (Grada). Praha: Grada Publishing. ISBN 978-80-247-4577-0.

GOLEMAN, Daniel, 2011. *Emoční inteligence*. Vyd. 2. Praha: Metafora, spol. s.r.o. ISBN 978-80-7359-334-6.

CHRÁSKA, Miroslav, 2016. *Metody pedagogického výzkumu: základy kvantitativního výzkumu*. 2., aktualizované vydání. Pedagogika (Grada). Praha: Grada Publishing. ISBN 978-80-247-53-263.

KLEPÁČKOVÁ, Olga; KREJČÍ, Zuzana a ČERNÁ, Martina, 2022. *Sociální práce na příkladech z praxe*. Praha: Grada Publishing. ISBN 978-80-271-4887-5.

KOLOUCH, Jan, 2016. *CyberCrime*. Praha: Edice CZ.NIC. ISBN 978-80-88168-16-4. Dostupné také z: <https://www.bookport.cz/kniha/cybercrime-5994/>.

KOPECKÝ, Kamil; SZOTKOWSKI, René a KREJČÍ, Veronika, 2015. *Rizikové formy chování českých a slovenských dětí v prostředí internetu*. Monografie. Olomouc: Univerzita Palackého v Olomouci. ISBN 978-80-244-4861-9.

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

KOŽÍŠEK, Martin, 2024. *Strážci na internetu*. CZ.NIC. ISBN 978-80-88168-73-7.

KRÁL, Mojmír, 2015. *Bezpečný internet: Chraňte sebe i svůj počítač*. Praha: Grada Publishing. ISBN 978-80-247-9821-9. Dostupné také z: <https://www.bookport.cz/kniha/bezpecny-internet-2473/>.

LANGMEIER, Josef a KREJČÍŘOVÁ, Dana, 2006. *Vývojová psychologie*. 2., aktualizované vydání. Psyché (Grada). Praha: Grada Publishing. ISBN 978-80-247-1284-0.

MAREŠ, Petr, 2022. *Kyberkultura, hackeři a digitální revoluce: Informace chce být svobodná*. Grada Publishing. ISBN 978-80-271-4899-8. Dostupné také z: <https://www.bookport.cz/kniha/kyberkultura-hackeri-a-digitalni-revoluce-10925/>.

MARTÍNEK, Zdeněk, 2015. *Agresivita a kriminalita školní mládeže*. 2., aktualizované a rozšířené vydání. Pedagogika. Praha: Grada Publishing. ISBN 978-80-247-5309-6.

SLUSSAREFF, Michaela, 2022. *Hry, síť, porno: Rodičovský průvodce džunglí digitálního dětství a puberty*. Brno: Jan Melvil Publishing. ISBN 978-80-7555-157-3.

SZOTKOWSKI, René; KOPECKÝ, Kamil a KREJČÍ, Veronika, 2013. *Nebezpečí internetové komunikace IV*. Olomouc: Univerzita Palackého v Olomouci. ISBN 978-80-244-3912-9.

ŠMAHEL, David, 2003. *Psychologie a internet: děti dospělými, dospělí dětmi*. Praha: Triton. ISBN 80-7254-360-1.

THOROVÁ, Kateřina, 2015. *Vývojová psychologie: proměny lidské psychiky od početí po smrt*. Praha: Portál. ISBN 978-80-262-0714-6.

VÁGNEROVÁ, Marie a LISÁ, Lidka, 2021. *Vývojová psychologie: dětství a dospívání*. Vydání třetí, přepracované a doplněné. Praha: Karolinum. ISBN 978-80-246-4961-0.

Zákony:

ČESKO, 2009. *Zákon č. 40/2009 Sb. trestní zákoník*. Online. In: *Zákony pro lidi*. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>. [cit. 2024-11-26].

Internetové zdroje:

5 způsobů krádeže hesel a jak se bránit, 2022. Online. Česká zemědělská univerzita v Praze. 10.1.2022. Dostupné z: <https://bezpecnost.czu.cz/cs/r-14483-aktuality-bezpecnost/5-zpusobu-kradeze-hesel-a-jak-se-branit.html>. [cit. 2025-02-13].

6 tipů, jak nenaletět fake news a hoaxům, b. r.. Online. O2 Chytrá škola. Dostupné z: <https://vyuka.o2chytraskola.cz/clanek/13/fake-news-deepfake-a-hoaxy/15009>. [cit. 2025-02-03].

Adware, c1992-2024. Online. Eset. Dostupné z: <https://www.eset.com/cz/adware/>. [cit. 2024-11-05].

Bílý kruh bezpečí, b. r.. Online. Dostupné z: <https://www.bkb.cz/>. [cit. 2025-04-09].

BRADÁČOVÁ, Kateřina, 2020. *Vliv youtuberů na děti mladšího školního věku*. Online, Diplomová práce, vedoucí Jana Marie Havigerová. Hradec Králové: Univerzita Hradec Králové, Pedagogická fakulta, Ústav primární a preprimární edukace. Dostupné z: <https://theses.cz/id/uaqct0/STAG90982.pdf>. [cit. 2025-02-05].

Bud' safe online, c2025. Online. Avast. Dostupné z: <https://www.avast.com/cz/besafeonline/>. [cit. 2025-04-09].

BURÝŠKOVÁ, Lenka, 2009. *Víte co je KYBERSÍKANA?* Online. Policie České republiky. 11. 12. 2009. Dostupné z: <https://www.policie.cz/clanek/vite-co-je-kybersikana.aspx>. [cit. 2024-10-16].

Co je flaming, 2008. Online. E-Bezpečí. 31. květen 2008. Dostupné z: <https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/dalsi-temata/38-co-je-flaming>. [cit. 2025-02-20].

Co je kybersíkana?, c2008-2024. Online. E-Bezpečí. Dostupné z: <https://www.e-bezpeci.cz/index.php/kontakt/71-trivium/1418-co-je-kybersikana>. [cit. 2024-10-16].

Co je počítačový virus + druhy virů, c1992-2024. Online. Eset. Dostupné z: <https://www.eset.com/cz/virus/>. [cit. 2024-11-05].

Co je to stalking a cyberstalking, 2008. Online. E-Bezpečí. 17. květen 2008. Dostupné z: <https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kyberstalking/66-23>. [cit. 2024-11-26].

Consequences of Sexting, c2025. Online. UPMC Children's Community Pediatrics. Dostupné z: <https://www.childrenspeds.com/health-resources/adolescent-health-and-wellness/sexting>. [cit. 2025-04-09].

Časopis Cyberpsychology, c2025. Online. Interdisciplinární výzkum internetu a společnosti – Masarykova univerzita. Dostupné z: <https://irtis.muni.cz/cs/casopis-cyberpsychology>. [cit. 2025-04-12].

Definition of Keyloggers, c2024. Online. Fortinet. Dostupné z: <https://www.fortinet.com/resources/cyberglossary/what-is-keyloggers>. [cit. 2024-11-05].

Digiděti, [2018]. Online. Dostupné z: <https://digideti.cz/>. [cit. 2025-04-12].

DOLEJŠ, Martin a OREL, Miroslav, 2017. *Rizikové chování u adolescentů a impulzivita jako prediktor tohoto chování*. Online. Olomouc: Univerzita Palackého v Olomouci. ISBN 978-80-244-5252-4. Dostupné z: <https://doi.org/10.5507/ff.17.24452524>. [cit. 2025-02-26].

E-Bezpečí, c2008-2024. Online. Dostupné z: <https://www.e-bezpeci.cz/>. [cit. 2025-04-09].

EVROPSKÁ KOMISE, 2022. *Pokyny pro učitele a další pracovníky ve výchově a vzdělávání, které se týkají boje proti dezinformacím a podpory digitální gramotnosti prostřednictvím vzdělávání a odborné přípravy*. Online. Lucemburk: Úřad pro publikace

Evropské unie. ISBN 987-92-76-55098-3. Dostupné z: <https://doi.org/10.2766/123007>. [cit. 2024-11-20].

FREED, Diana; BAZAROVA, Natalie N.; CONSOLVO, Sunny; HAN, Eunnice J.; KELLEY, Patrick G. et al., 2023. Understanding Digital-Safety Experiences of Youth in the U.S. Online. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 2023-04-19, vol. 23, no. 191, s. 1-15. ISBN 9781450394215. Dostupné z: <https://doi.org/10.1145/3544548.3581128>. [cit. 2025-03-24].

FRÝDECKÁ, Lucie, 2009. *Nebezpečné pronásledování*. Online. Bílý Kruh Bezpečí. 21.4.2009. Dostupné z: <https://www.bkb.cz/pomoc-obetem/trestne-ciny/nebezpecne-pronasledovani/>. [cit. 2024-11-26].

GAJDOŠOVÁ, Jana, 2011. *Zdravotní a psychické následky kyberšikany mezi dětmi a dospívající mládeží*. Online. E-Bezpečí. 17. listopad 2011. Dostupné z: <https://www.e-bezpeci.cz/index.php/temata/dali-rizika/355-zdravotni-a-psychicke-nasledky-kyberikany-mezi-dtmi-a-dospivajici-mladei?>. [cit. 2025-02-20].

Happy slapping, 2008. Online. E-Bezpečí. 15. listopad 2008. Dostupné z: <https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kybersikana/87-71>. [cit. 2025-02-20].

HAŠLOVÁ, Eva, 2020. *Na internetu s obezřetností*. Online. Policie ČR. 12.3. 2020. Dostupné z: <https://www.policie.cz/clanek/na-internetu-s-obezretnosti.aspx>. [cit. 2024-11-26].

HOAX, 2016. Online. E-Bezpečí. 11. říj. 2016. Dostupné z: <https://www.e-bezpeci.cz/index.php/ke-stazeni/tiskoviny/bud-v-bezpeci/90-bud-v-bezpeci-hoax/file>. [cit. 2024-11-20].

HOLCOVÁ, Šárka, 2019. *Rizikové formy chování pubescentů a adolescentů v prostředí internetu*. Online, Diplomová práce, vedoucí Albín Škoviera. Pardubice: Univerzita Pardubice, Fakulta filozofická. Dostupné z: <https://dk.upce.cz/server/api/core/bitstreams/e427b413-3e93-4059-9e3c-3cee96b1d427/content>. [cit. 2025-04-09].

HOLLÁ, Katarína, 2021. *Riziká kyberšikanovania a sextingu a možnosti prevencie*. Online. Národné osvetové centrum. 27. 7. 2021. Dostupné z: <https://www.nocka.sk/rizika-kybersikanovania-a-sextingu-a-moznosti-prevencie/>. [cit. 2024-10-23].

HYKYŠOVÁ, Alena, 2019. České děti se chodí na internet bavit. Online. *Statistika&my*. Roč. 9, č. 03, s. 25-26. Dostupné z: <https://statistikaamy.csu.gov.cz/docs/107903/0c3fb3bb-b01c-9862-65cf-d0a8e3286eaa/18041903.pdf?version=1.0>. [cit. 2025-03-03].

Influenceri: vlivní kreativci z internetu, 2022. Online. České překlady. 30. 8. 2022. Dostupné z: <https://www.ceskepreklady.cz/influenceri/>. [cit. 2025-02-10].

Informace o projektu - E-bezpečí, c2008-2024. Online. E-Bezpečí. Dostupné z: <https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu>. [cit. 2024-11-04].

Jak se chránit před kyberšikanou a jak se bránit kyberútočníkům, 2009. Online. E-Bezpečí. 22. květen 2009. Dostupné z: <https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kybersikana>. [cit. 2025-02-22].

JANDOVÁ, Regina, c1994–2025. *Co dělat, když je vaše dítě obětí kyberšikany?* Online. Linka bezpečí. Dostupné z: <https://www.linkabezpeci.cz/-/co-delat-kdyz-je-vase-dite-obeti-kybersikany>. [cit. 2025-02-22].

JANSEN, Helen Almind; WODSCHOW, Anne a MADSEN, Svend Aage, 2011. PSYCHOLOGICAL TREATMENT OF CHILDREN SEXUALLY ABUSED DUE TO A CONTACT ON THE INTERNET. Online. *Ontario Association of Children's Aid Societies JOURNAL*. Vol. 56, no. 3, s. 22-29. Dostupné z: <https://www.rigshospitalet.dk/afdelinger-og-klinikker/julianemarie/center-for-seksuelle-overgreb/for-fagfolk/Documents/helene-jansen-psykologisk-behandling-af-boern.pdf>. [cit. 2025-04-09].

Kdo je to Youtuber?, c2008-2024. Online. IT-slovník. Dostupné z: <https://it-slovník.cz/pojem/youtuber>. [cit. 2025-02-05].

KOĐOUSKOVÁ, Barbora, 2024. *HTTPS v kostce: co to je, jak funguje a jak na něj přejít*. Online. Rascasone. 03/07/2024. Dostupné z: <https://www.rascasone.com/cs/blog/co-je-https-http-ssl-tls>. [cit. 2025-02-03].

KOHOUT, Roman, 2017a. *Krádež identity*. Online. Internetem Bezpečně. 14.7.2017. Dostupné z: <https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/kradez-identity/>. [cit. 2025-02-18].

KOHOUT, Roman, 2017b. *Pořizování záznamů za účelem poškodit oběť*. Online. Internetem Bezpečně. 26.7.2017. Dostupné z: <https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/porizovani-zaznamu-za-ucelem-poskodit-obet/>. [cit. 2025-02-18].

KOPECKÝ, Kamil, 2010. *Nebezpečí zvané kybergrooming II – metody manipulace*. Online. In: Národní pedagogický institut České republiky, Metodický portál RVP.CZ. 30. 11. 2010. Dostupné z: <https://clanky.rvp.cz/clanek/c/OUG/9985/NEBEZPECI-ZVANE-KYBERGROOMING-II---METODY-MANIPULACE.html>. [cit. 2024-11-26].

KOPECKÝ, Kamil, 2022a. *Co je to vlastně ten hoax, dezinformace, misinformace nebo třeba fake news? Čím se tyto termíny liší a co mají společného?* Online. E-Bezpečí. 2. listopad 2022. Dostupné z: <https://www.e-bezpeci.cz/index.php/clanky-komentare/2864-co-je-to-vlastne-ten-hoax-dezinformace-misinformace-nebo-treba-fake-news-cim-se-tyto-termíny-lisi-a-co-maji-spolecneho>. [cit. 2024-11-20].

KOPECKÝ, Kamil, 2022b. *Základy fact-checkingu*. Online. E-Bezpečí. Dostupné z: <https://e-bezpeci.cz/factchecking/>. [cit. 2025-02-03].

KOPECKÝ, Kamil, 2024. *Digitální závislost: Fenomén současnosti*. Online. E-Bezpečí. 10. červen 2024. Dostupné z: <https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/online-zavislosti/4067-digitalni-zavislost-fenomen-soucasnosti>. [cit. 2024-11-21].

KOPECKÝ, Kamil, c2007-2024. *KYBERGROOMING: rizikové seznamování v online prostředí*. Online. E-bezpečí. Dostupné z: <https://www.e-bezpeci.cz/kybergrooming/>. [cit. 2024-10-22].

KOPECKÝ, Kamil, c2008-2024a. *DESATERO BEZPEČNÉHO CHOVÁNÍ NA INTERNETU OD E-BEZPEČÍ*. Online. E-Bezpečí. Dostupné z: <https://www.e-bezpeci.cz/desatero/>. [cit. 2025-01-21].

KOPECKÝ, Kamil, c2008-2024b. *NETOLISMUS*. Online. E-Bezpečí. Dostupné z: <https://www.e-bezpeci.cz/netolismus/>. [cit. 2024-11-21].

KUBALA, Lukáš, 2019. *Facebook umírá, žezlo přebírá Instagram*. Online. E-Bezpečí. 18. leden 2019. Dostupné z: <https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/socialni-site/1440-facebook-umira-zezlo-prebira-instagram>. [cit. 2025-01-21].

KYSELÁ, Iva, 2019. *Puberta dítěte a jak ji zvládnout*. Online. Akademie rodičovství. 14.6.2019. Dostupné z: <https://www.akademierodicovstvi.cz/blog/puberta-ditete-a-jak-ji-zvladnout?>. [cit. 2025-02-25].

LAMB-HALL, Malea, 2023. *Jak na online randění: 5 tipů, díky kterým se seznámíte bezpečně!*. Online. Avast blog. 12 Úno 2023. Dostupné z: <https://blog.avast.com/cs/5-tipu-na-bezpecne-seznamovani>. [cit. 2025-01-23].

Linka bezpečí, c1994–2025. Online. Dostupné z: <https://www.linkabezpeci.cz/>. [cit. 2025-04-09].

MARTINEK, Petr a KOSOVÁ, Lucie, c2025. *Kyberstalking 1*. Online. Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: <https://osveta.nukib.gov.cz/mod/page/view.php?id=1121>. [cit. 2025-02-18].

MIOVSKÝ, Michal; SKÁCELOVÁ, Lenka; ČÁBLOVÁ, Lenka; VESELÁ, Michaela a ZAPLETALOVÁ, Jana, 2012. *Návrh doporučené struktury minimálního preventivního programu prevence rizikového chování por základní školy*. Online. Praha: Univerzita Karlova v Praze & TOGGA. ISBN 987-80-87258-74-3. Dostupné z: <https://www.adiktologie.cz/file/331/minim-prevent-program-web.pdf>. [cit. 2025-04-12].

MŠMT, c2013 – 2025. *Metodická doporučení a metodické pokyny*. Online. MŠMT. Dostupné z: <https://msmt.gov.cz/vzdelavani/socialni-programy/metodicke-dokumenty-doporuceni-a-pokyny>. [cit. 2025-04-11].

PETRÁKOVÁ, Hana, c1994–2024. *Sociální sítě a duševní zdraví mohou být v symbióze*. Online. Linka bezpečí. Dostupné z: <https://www.linkabezpeci.cz/-/socialni-site-a-dusevni-zdravi>. [cit. 2024-12-03].

Phishing, c1992-2024. Online. Eset. Dostupné z: <https://www.eset.com/cz/phishing/>. [cit. 2024-11-05].

PREECE, Tamasine, 2017. *How are YouTubers influencing children?* Online. Internet Matters. Dostupné z: <https://www.internetmatters.org/hub/expert-opinion/youtubers-influencing-children/>. [cit. 2024-11-19].

PRICE, Megan a DALGLEISH, John, 2010. Cyberbullying : Experiences, impacts and coping strategies as described by Australian young people. Online. *Youth Studies Australia*. Vol. 29, no. 2, s. 51-59. ISSN 1038-2569. Dostupné z: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=14258669734d9f9db33da9ed8da9647f415d7dda>. [cit. 2025-03-24].

Ransomware, c2018. Online. Internetem Bezpečně. Dostupné z: <https://www.internetembezpecne.cz/internetem-bezpecne/malware/ransomware/>. [cit. 2024-11-05].

REDAKCE RADINET.CZ, 2024. *Jak vytvořit bezpečné prostředí pro děti v digitálním věku*. Online. Rodinet.cz. 24. 10. 2024. Dostupné z: <https://www.rodinet.cz/jak-vytvorit-bezpecne-prostredi-pro-deti-v-digitalnim-veku-2/>. [cit. 2025-02-13].

REDAKCE SITEVHRSTI.CZ, 2020. *Nejznámější a nejoblíbenější sociální sítě v ČR*. Online. Sítě v hrsti. 26. 10. 2020. Dostupné z: <https://sitevhrsti.cz/nejoblibenejsi-socialni-site-cr/>. [cit. 2025-02-11].

Replug me, [2020]. Online. Dostupné z: <https://www.replug.me/>. [cit. 2025-04-11].

RYBÁŘOVÁ, Alžběta, 2020. *Sociální sítě jako fenomén dnešní doby*. Online. Marianne. 6. 11. 2020. Dostupné z: <https://www.marianne.cz/zivotni-styl/vite-kdo-je-influencer-youtuber-nebo-tiktoker?>. [cit. 2025-02-10].

SMAHEL, David; MACHACKOVA, Hana; MASCHERONI, Giovanna; DEDKOVA, Lenka; ÓLAFSSON, Kjartan et al., 2020. *EU Kids Online 2020: Survey results from 19 countries*. Online. *EU Kids Online*. S. 1-157. ISSN 2045-256X. Dostupné z: <https://doi.org/10.21953/lse.47fdeqj01ofo>. [cit. 2025-04-09].

Sociální sítě, b. r.. Online. MarketingPPC. Dostupné z: <https://www.marketingppc.cz/ppc/socialni-site/>. [cit. 2024-12-02].

Sociální sítě, c2018. Online. Internetem Bezpečně. Dostupné z: <https://www.internetembezpecne.cz/internetem-bezpecne/socialni-media/socialni-site/>. [cit. 2024-12-03].

Sociální sítě, c2024. Online. Sítě v hrsti. Dostupné z: <https://sitevhrsti.cz/socialni-site/>. [cit. 2024-12-02].

SOURANDER, Andre; BRUNSTEIN KLOMEK, Anat; IKONEN, Maria; LINDROOS, Jarna; LUNTAMO, Terhi et al., July 2010. *Psychosocial Risk Factors Associated With Cyberbullying Among Adolescents*. Online. *Archives of General Psychiatry*. Roč. 67, č. 7. ISSN 0003-990X. Dostupné z: <https://doi.org/10.1001/archgenpsychiatry.2010.79>. [cit. 2025-02-20].

Spam, c1992-2024. Online. Eset. Dostupné z: <https://www.eset.com/cz/spam/>. [cit. 2024-11-20].

Spyware, c1992-2024. Online. Eset. Dostupné z: <https://www.eset.com/cz/spyware/>. [cit. 2024-11-05].

Streamer/ka, b. r.. Online. Visibility. Dostupné z: <https://visibility.sk/blog/slovník/streamer/>. [cit. 2025-02-12].

ŠIMEK, Gabriel, 2022. *5 sociálních sítí dominujících v roce 2022*. Online. Life24.cz. 04.05.2022. Dostupné z: <https://www.life24.cz/technologie/5-socialnich-siti-dominujicich-v-roce-2022>. [cit. 2025-02-11].

ŠPELDA, David, 2020. *Kyberšikana, její prevence a vyšetřování; psychologické, technické a právní aspekty problému*. Online, Diplomová práce, vedoucí Michal Musílek. Hradec Králové: Univerzita Hradec Králové, Pedagogická fakulta, Katedra aplikované kybernetiky Přírodovědecké fakulty. Dostupné z: <https://theses.cz/id/a8kz7n/STAG91972.pdf>. [cit. 2025-04-09].

Trojský kůň, c1992-2024. Online. Eset. Dostupné z: <https://www.eset.com/cz/trojsky-kun/>. [cit. 2024-11-05].

VOHANKOVÁ, Alena, 2020. *Poslal/a jsem nahé fotky a vydírá mě, co mám dělat?* Online. Buď safe online. 20. 2. 2020. Dostupné z: <https://www.avast.com/cz/besafeonline/blog/poslal-a-jsem-nahe-fotky-a-vydira-me-co-mam-delat>. [cit. 2025-02-05].

WESTENBERG, Wilma, 2016. *The influence of YouTubers on teenagers : a descriptive research about the role YouTubers play in the life of their teenage viewers*. Online. University of Twente. Dostupné z: <https://essay.utwente.nl/71094/>. [cit. 2025-02-05].

WHITTLE, Helen; HAMILTON-GIACHRITSIS, Catherine; BEECH, Anthony a COLLINGS, Guy, 2013. A review of young people's vulnerabilities to online grooming. Online. *Aggression and Violent Behavior*. Roč. 18, č. 1, s. 135-146. ISSN 1359-1789. Dostupné z: <https://www.sciencedirect.com/science/article/abs/pii/S135917891200122X>. [cit. 2025-03-24].

YOUTUBE, c2024. Online. Sítě v hrsti. Dostupné z: <https://sitevhrsti.cz/socialni-site/youtube/>. [cit. 2024-11-19].

ZDRAVOTNICKÁ ZÁCHRANNÁ SLUŽBA OLOMOUCKÉHO KRAJE P.O. [@zss.ok], 2025. *Nebezpečná výzva z TikToku*. Online. Dostupné z:

Instagram, <https://www.instagram.com/p/DFvNnbUMKUd/?igsh=M240bXRua3Nwa2ww>.
[cit. 2025-02-12].

SEZNAM OBRÁZKŮ

Obrázek 1 Ukázka spamu	30
Obrázek 2 Losování kraje	44
Obrázek 3 Losování okresu	44

SEZNAM TABULEK

Tabulka 1 Seznam krajů dle čísel	43
Tabulka 2 Seznam okresů Olomouckého kraje dle čísel	44

SEZNAM GRAFŮ

Graf 1 Znalost rizik.....	48
Graf 2 Zdroj informací o rizicích.....	48
Graf 3 Vnímání komunikace s cizími lidmi na internetu.....	49
Graf 4 Platformy pro komunikaci s cizími lidmi.....	50
Graf 5 Vyžadování osobních informací cizím člověkem	51
Graf 6 Návrh osobní schůzky	51
Graf 7 Luring	52
Graf 8 Nepřímé setkání s nenávisťnými komentáři	53
Graf 9 Reakce na nenávisťné komentáře.....	55
Graf 10 Příjem pornografického materiálu.....	55
Graf 11 Šíření (vlastního) pornografického materiálu.....	56
Graf 12 Nadměrný zájem a kontrola jiným uživatelem.....	57
Graf 13 Výskyt dezinformací	57
Graf 14 Šíření dezinformací	58
Graf 15 Důvěra v osoby na sociálních sítích	58
Graf 16 Vliv osob vystupujících na internetu.....	59
Graf 17 Rizika spojená se sledováním osob vystupujících na internetu.....	60
Graf 18 Sdílení osobních údajů na internetu	60
Graf 19 Pocit bezpečí.....	61
Graf 20 Pocity u luringu	62
Graf 21 Pocity při setkání s phishingem.....	63
Graf 22 Pocit při stažení malwaru	63
Graf 23 Vlastní pocity při zesměšnění či urážení	65
Graf 24 Pocity při setkání s pornografickým obsahem.....	66
Graf 25 Pocity při nadměrném zájmu jiným uživatelem.....	67
Graf 26 Pocity při setkání s dezinformací	68
Graf 27 Reakce na zprávu od cizí osoby	68
Graf 28 Zveřejňování informací s rizikem ovlivnění do budoucna.....	69
Graf 29 Žádost o přátelství nebo sledování cizími lidmi.....	70
Graf 30 Prevence z pohledu pubescentů.....	71
Graf 31 Zdroj informací o digitální bezpečnosti	71
Graf 32 Pocit vzdělanosti o bezpečnosti v digitálním světě	72
Graf 33 Vnímání informovanosti o bezpečnosti ze strany rodičů či školy.....	73

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

%	procento
§	paragraf
ad.	a další
apod.	a podobně
atp.	a tak podobně
b.r.	bez roku
Bc.	Akademický titul – absolvent vysoké školy v bakalářském studijním programu
ČR	Česká republika
EU	Evropská unie
HTTPS	Hypertext Transfer Protocol Secure
ICT	informační a komunikační technologie
MŠMT	Ministerstvo školství, mládeže a tělovýchovy
např.	například
OSPOD	Orgán sociálně-právní ochrany dětí
PIN	personal identification number
Sb.	Sbírka zákonů
SMS	služba krátkých textových zpráv
tnz.	to znamená
tzv.	takzvaně
USA	Spojené státy americké

SEZNAM PŘÍLOH

Příloha P I: Dotazník

Příloha P 2: Položky v dotazníku a výzkumné otázky

PŘÍLOHA P I: DOTAZNÍK

31.03.25 12:26

POHLED ŽÁKŮ NA BEZPEČNOST V DIGITÁLNÍM SVĚTĚ

POHLED ŽÁKŮ NA BEZPEČNOST V DIGITÁLNÍM SVĚTĚ

Vážený žaku,

jmenuji se Gabriela Klágová a jsem studentkou 3. ročníku oboru Sociální pedagogika na Univerzitě Tomáše Bati ve Zlíně. Tento dotazník jsem vytvořila, abych lépe porozuměla tomu, jak se žáci cítí v digitálním prostředí, jaké bezpečnostní rizika znají, se kterými riziky mají zkušenost a jak chrání své soukromí online. Tvé odpovědi budou velmi cenným zdrojem pro lepší pochopení a zlepšení opatření na ochranu online bezpečnosti mladých lidí.

Tento dotazník je určen žákům základních škol nebo gymnázií ve věku **11-15 let**.

Zdůrazňuji, že tvá účast je **dobrovolná** a všechny získané informace budou zpracovány **anonymně a důvěrně**. Tvé odpovědi budou použity pouze pro účely této výzkumné studie a nebudou šířeny žádným jiným způsobem.

Dotazník je jednoduchý – zaklikni **jednu odpověď**, případně **více** tam, kde je to uvedeno, nebo **napiš odpověď** do vymezeného prostoru.

Děkuji ti za tvůj čas a zapojení se do této důležité studie.

S pozdravem,

Gabriela Klágová

* Označuje povinnou otázku

1. Pohlaví *

Označte jen jednu elipsu.

☐ Dívka

☐ Chlapec

2. Kolik je ti let? *

Použij pouze číslice

3. Jaké typy digitálních rizik znáš? *

*Vyber jednu nebo více odpovědí**Zaškrtněte všechny platné možnosti.*

- ☐ Kyberšikana (šikana prováděná prostřednictvím digitálních technologií)
- ☐ Kybergrooming (manipulace, obtěžování online)
- ☐ Stalking a kyberstalking (opakované a nevyžádané sledování nebo obtěžování osoby)
- ☐ Dezinformace (záměrně šířené nepravdivé informace)
- ☐ Sexting (posílání fotek nebo zpráv s nahými nebo sexuálními tématy přes internet)
- ☐ Phishing (podvod, kdy se někdo snaží získat tvoje osobní údaje pomocí falešných e-mailů nebo webů)
- ☐ Malware (škodlivý software, který poškozuje počítače nebo krade informace)
- ☐ Luring (lákání oběti k osobnímu setkání za účelem zneužití)
- ☐ Jiné: _____

4. Kde jsi se o těchto rizicích dozvěděl/la? *

*Vyber jednu nebo více odpovědí**Zaškrtněte všechny platné možnosti.*

- ☐ Od kamarádů či spolužáku
- ☐ Ve škole
- ☐ Z vlastních zkušeností
- ☐ Od rodičů
- ☐ Na internetu (YouTube videa, sociální sítě, ...)
- ☐ Jiné: _____

5. Chováš se na internetu bezpečně? *

Označte jen jednu elipsu.

- ☐ Ano
- ☐ Ne

6. Cítíš se na internetu v bezpečí? *

Označte jen jednu elipsu.

- ☐ Rozhodně ano
- ☐ Spíše ano
- ☐ Spíše ne
- ☐ Rozhodně ne

7. Je podle tebe komunikace na internetu s lidmi, které neznáš, bezpečná? *

Označte jen jednu elipsu.

- ☐ Rozhodně ano
- ☐ Spíše ano
- ☐ Nevím
- ☐ Spíše ne
- ☐ Rozhodně ne

8. Komunikuješ na internetu s lidmi, které neznáš? (např. na sociálních sítích, při hraní her) *

Označte jen jednu elipsu.

- ☐ Ano
- ☐ Ne

9. **Pokud ano, na jakých platformách s nimi komunikuješ? ***

Vyber jednu nebo více odpovědí

Zaškrtněte všechny platné možnosti.

- ☐ YouTube
- ☐ Facebook (Messenger)
- ☐ Při hraní her
- ☐ Snapchat
- ☐ Instagram
- ☐ Discord/TeamSpeak/Skype
- ☐ E-mail
- ☐ Twitch
- ☐ TikTok
- ☐ X (Twitter)
- ☐ Diskuzní fóra (např. Reddit)
- ☐ WhatsApp
- ☐ Nekomunikuji s nikým neznámým
- ☐ Jiné: _____

10. Setkal/a jsi se někdy s někým v online prostoru, kdo ti psal hodně osobní zprávy? *

Označte jen jednu elipsu.

- ☐ Ano
- ☐ Ne

11. Vyžadoval od tebe někdy někdo v online prostoru hodně osobní informace? *

Označte jen jednu elipsu.

- ☐ Ano, ale nesdělil/a jsem mu žádné osobní informace
- ☐ Ano a sdělil/a jsem mu je dobrovolně
- ☐ Ano a sdělil/a jsem mu je pod nátlakem
- ☐ Ne

12. Navrhl ti někdy člověk, kterého neznáš osobně, přes internet osobní schůzku? *

Označte jen jednu elipsu.

- ☐ Ano, šel/šla jsem na ni
- ☐ Ano, ale nedorazil/la jsem
- ☐ Ne

13. Napsal ti někdy někdo cizí na internetu podobnou zprávu? *
- „neříkej to rodičům, nepochopí to“ nebo „pokud jim to prozradíš, budeš mít problémy“*

Označte jen jednu elipsu.

- ☐ Ano
- ☐ Ne

14. Nabízel ti někdo něco (peníze, nový telefon, oblečení, novou počítačovou hru) za to, že mu pošleš například své telefonní číslo, adresu bydliště nebo jiné podobné informace? *

Označte jen jednu elipsu.

- ☐ Ano, dala jsem mu je dobrovolně
- ☐ Ano, dala jsem mu je pod nátlakem (vyhrožoval mi)
- ☐ Ano, ale nedal/a jsem mu je
- ☐ Ne

15. **Pokud ano** - Jak jsi se cítil/la, když jsi dostal/a nabídku, ve které ti osoba nabízela dárky výměnou za osobní informace? *

Vyber jednu nebo více odpovědí

Zaškrtněte všechny platné možnosti.

- ☐ Cítil/a jsem vztek, protože jsem nevěděl/a, že je to podvod.
- ☐ Měl/a jsem strach z nebezpečí.
- ☐ Cítil/a jsem se nervózně.
- ☐ Cítil/a jsem se zoufale, nevěděl/a jsem, co mám dělat.
- ☐ Pobavilo mě, jak někdo může zkoušet takové triky.
- ☐ Cítil/a jsem důvěru, protože to vypadalo jako něco, co by mohlo být v pořádku.
- ☐ Překvapilo mě, že mi někdo něco takového nabízí.
- ☐ Znechutilo mě, že někdo může takhle zneužívat důvěru druhých.
- ☐ Připadal/a jsem si provinile, že jsem tomu na chvíli věřil/a.
- ☐ Měl/a jsem radost, že jsem se nenechal/a nachytat.
- ☐ Nikdy se mi to nestalo.
- ☐ Jiné: _____

16. Přišel ti někdy e-mail, který se ti zdál podezřelý? (byl od cizí osoby, zvláštní text, * obsahoval odkaz)

Označte jen jednu elipsu.

- ☐ Ano
- ☐ Ne
- ☐ Nevybavuji si

17. **Pokud ano** - Jak se cítíš, když obdržíš podezřelý e-mail? **Vyber jednu nebo více odpovědí**Zaškrtněte všechny platné možnosti.*

- ☐ Cítím vztek, protože mě štví, že někdo posílá takové věci.
- ☐ Jsem znechucený/á, že se to stále děje.
- ☐ Cítím se zoufale, protože nevím, co s tím dělat.
- ☐ Jsem nervózní, abych na něco špatně neklikl/la nebo neotevřel/la něco.
- ☐ Jsem v šoku, že něco takového někdo posílá.
- ☐ Stydím se, že jsem mu možná na začátku trochu uvěřil/a.
- ☐ Pobaví mě to, protože je to blbost.
- ☐ Mám radost, že jsem podezřelý e-mail poznal/a a nepodleh/a tomu.
- ☐ Nikdy jsem neobdržel/a nebo si nejsem jistý/á.
- ☐ Jiné: _____

18. Klikl/a jsi někdy na odkaz, který ti přišel od kohokoliv, přitom jsi nevěděl/a, co se v odkaze nachází? *

Označte jen jednu elipsu.

- ☐ Ano, omylem
- ☐ Ano, úmyslně
- ☐ Ne

19. Podařilo se ti někdy omylem stáhnout nějaký druh malwaru? (např. virus, trojský kůň, adware atd.) *

Označte jen jednu elipsu.

- ☐ Ano
- ☐ Ne
- ☐ Nevím o tom, je to možné

20. **Pokud ano** - Jak jsi se cítil/a, když jsi zjistil/a, že máš v počítači malware? *
(např. virus, trojský kůň, adware atd.)

Vyber jednu nebo více odpovědí

Zaškrtněte všechny platné možnosti.

- ☐ Byl/a jsem naštvaný/á.
- ☐ Měl/a jsem strach, že ztratím své soubory na počítači.
- ☐ Cítil/a jsem zklamání, že jsem se stal/a obětí něčeho takového.
- ☐ Byl/a jsem v šoku.
- ☐ Cítil/a jsem znechucení, že mi něco takového vlezlo do počítače.
- ☐ Cítil/a jsem se trapně, že jsem nedal/a pozor.
- ☐ Nikdy se mi to nestalo nebo si nejsem jistý/á.

21. Viděl/a jsi nějaké nenávistné komentáře například pod příspěvky na sociálních *
sítích?

Označte jen jednu elipsu.

- ☐ Ano, velmi často
- ☐ Občas zahlédnu
- ☐ Ne, nikdy
- ☐ Nečtu si komentáře
- ☐ Nenavštěvuji sociální sítě

22. Přišel ti někdy nenávistný komentář pod tvůj příspěvek? (fotka či video na *
sociálních sítích)

Označte jen jednu elipsu.

- ☐ Ano
- ☐ Ne
- ☐ Nenavštěvuji sociální sítě

23. Napsal/a jsi ty někdy takový komentář? *

Označte jen jednu elipsu.

- ☐ Ano
- ☐ Ne
- ☐ Nenavštěvuji sociální sítě

24. Jak reaguješ na nenávistné komentáře, které vidíš pod příspěvky na sociálních sítích? *

Vyber jednu nebo více odpovědí

Zaškrtněte všechny platné možnosti.

- ☐ Cítím vztek, nelíbí se mi to.
- ☐ Zůstanu v šoku, že je někdo tak zlý.
- ☐ Cítím se sklesle, protože to kazí náladu.
- ☐ Snažím se to ignorovat, neřeším to.
- ☐ Pobaví mě to.
- ☐ Lituji, že jsem to vůbec četl/a.
- ☐ Snažím se podpořit toho, kdo je terčem nenávisti.
- ☐ Radši mlčím, protože nechci být terčem.
- ☐ Napíšu něco milého, abych vyvážil/a negativitu.
- ☐ Nečtu si komentáře.
- ☐ Nenavštěvuji sociální sítě.
- ☐ Jiné: _____

25. Jak se cítíš, když tě někdo na internetu uráží nebo zesměšňuje? *

Vyber jednu nebo více odpovědí

Zaškrtněte všechny platné možnosti.

- ☐ Cítím vztek a mám chuť jim něco vrátit.
- ☐ Cítím se smutně, protože mě to zasáhne.
- ☐ Mám strach, že se to bude opakovat nebo že se to zhorší.
- ☐ Jsem spokojený/á, když dokážu na urážky nereagovat.
- ☐ Překvapuje mě, jak daleko jsou lidé schopni zajít na internetu.
- ☐ Jsem znechucený/á tím, jak jsou někteří lidé zlí.
- ☐ Připadám si ponížene.
- ☐ Nikdy se mi to nestalo.
- ☐ Nemám sociální sítě.
- ☐ Jiné: _____

26. Byla ti někdy zaslána pornografická fotografie nebo video? (tzn. fotka či video, kde se nachází nahota) *

Označte jen jednu elipsu.

- ☐ Ano, jednou
- ☐ Ano, párkrát
- ☐ Ano, chodí mi často
- ☐ Ne, nikdy jsem se s tím nesetkal/a
- ☐ Ne, ale znám někoho, komu ano

27. **Pokud ano** - Jak se cítíš po setkání s pornografickým obsahem, kterému ses nechtěně vystavil/a? *

Vyber jednu nebo více odpovědí

Zaškrtněte všechny platné možnosti.

- ☐ Cítím vztek, nelíbilo se mi, že mi to někdo poslal.
- ☐ Cítím se znechuceně, nelíbilo se mi to.
- ☐ Jsem šokovaný/á a překvapený/á, že se mi něco takového objevilo.
- ☐ Cítím se zahanbeně.
- ☐ Cítím se smutně, nevím, jak to zpracovat.
- ☐ Jsem vyděšený/á nebo nervózní, že se mi to stalo.
- ☐ Je mi to jedno a nijak mě to neovlivnilo.
- ☐ Cítím se pobaveně nebo zvědavě, i když vím, že bych to neměl/a vidět.
- ☐ Snažím se na to zapomenout a ignorovat to.
- ☐ Je mi trapně, že jsem se do této situace dostala, i když jsem nechtěla.
- ☐ Nikdy jsem se s tím nesetkal/a.
- ☐ Jiné: _____

28. Poslal/a jsi někdy sám/sama fotku či video sebe, kde se nachází nahota? *

Označte jen jednu elipsu.

- ☐ Ano, dobrovolně
- ☐ Ano, pod nátlakem (vyhrožování, manipulace)
- ☐ Ne, nikdy jsem to neudělal/a
- ☐ Ne, ale znám někoho, kdo ano

29. Měl/a jsi někdy pocit, že ti někdo neustále psal, komentoval tvoje příspěvky nebo se o tebe zajímal víc, než bylo ti příjemné? *

Označte jen jednu elipsu.

- ☐ Ano, stalo se mi to a nelíbilo se mi to
- ☐ Ano, někdo se o mě víc zajímal, ale necítil/a jsem se nijak ohrožený/á
- ☐ Ano, ale řekl/la jsem, že s ním nechci komunikovat
- ☐ Ne, nikdy se to nestalo.
- ☐ Ne, ale stalo se to někomu, koho znám

30. **Pokud ano** - Jak ses cítil/la, když ti někdo psal nebo tě kontroloval víc, než bylo pro tebe příjemné? *

Vyber jednu nebo více odpovědí

Zaškrtněte všechny platné možnosti.

- ☐ Cítil/a jsem se nepříjemně, naštvalo mě to.
- ☐ Cítil/a jsem se zoufale, nevěděl/a jsem co mám dělat.
- ☐ Měl/a jsem obavy, že mě chce někdo sledovat.
- ☐ Pobavilo mě to, bylo to přehnané.
- ☐ Byl/a jsem v šoku.
- ☐ Připadalo mi to zvláštní, ale necítil/a jsem se ohrožený/á.
- ☐ Cítil/a jsem se a ztrapněný/á, měl/a jsem pocit neustálého sledování a kontroly.
- ☐ Nelíbilo se mi to, protože to bylo zasahování do mého soukromí.
- ☐ Nikdy se mi to nestalo.
- ☐ Jiné: _____

31. Dostal/a jsi někdy zprávu, která obsahovala informaci, o které jsi později zjistil/a, že byla nepravdivá? *

Označte jen jednu elipsu.

- ☐ Ano, několikrát
- ☐ Ano, jednou
- ☐ Ne, nikdy

32. **Pokud ano** - Jak ses cítil/la, když jsi zjistil/a, že informace, kterou jsi dostal/anebo sdílel/a, byla nepravdivá? *

Vyber jednu nebo více odpovědí

Zaškrtněte všechny platné možnosti.

- ☐ Cítil/a jsem se otráveně nebo jsem měl/a vztek.
- ☐ Bylo mi to líto, protože jsem věřil/a něčemu, co bylo nepravdivé.
- ☐ Měl/a jsem obavy.
- ☐ Cítil/a jsem úlevu, protože jsem se z toho nakonec dostal/a bez problémů a vzal/a si z toho ponaučení.
- ☐ Překvapilo mě, že jsem mohl/a být tak snadno oklamán/a
- ☐ Bylo mi z toho zle, protože jsem měl/a pocit, že se se mnou někdo snaží manipulovat.
- ☐ Cítil/a jsem se ponížený/á, že jsem uvěřil/a něčemu, co nebylo pravda.
- ☐ Necítil/a jsem se nijak zvlášť, prostě se to stalo.
- ☐ Nikdy se mi to nestalo.
- ☐ Jiné: _____

33. Sdílel/a jsi někdy online informaci, u které jsi později zjistil/a, že byla nepravdivá? *

Označte jen jednu elipsu.

- ☐ Ano, několikrát
- ☐ Ano, ale jen jednou
- ☐ Ne, nikdy

34. Důvěřuješ informacím, které sdílí tví oblíbení YouTuberi/influenceri/streamerři? *

Označte jen jednu elipsu.

- ☐ Ano, vždy jim věřím
- ☐ Částečně, přemýšlím o tom, co sdílí a pokud to jde, ověřuji si informace
- ☐ Ne, beru jejich obsah spíše jako zábavu než zdroj seriózních informací
- ☐ Záleží na tématu – někdy věřím, někdy ne

35. Jaký si myslíš, že mají na tebe vliv osoby na internetu (influenceri, YouTuberi, streameri)? *

Označte jen jednu elipsu.

- ☐ Velký, často se inspiroji jejich názory nebo stylem.
- ☐ Střední, některé jejich názory mě zajímají, ale většinou zachovám vlastní názor.
- ☐ Malý, sleduji je spíše pro zábavu.
- ☐ Žádný, rozhodnutí dělám podle sebe.

36. Jaká rizika podle tebe mohou být spojena s tím, že lidé sledují tyto osoby? *

Vyber jednu nebo více odpovědí

Zaškrtněte všechny platné možnosti.

- ☐ Sdílení nepravdivých nebo zavádějících informací, které mohou ovlivnit rozhodování.
- ☐ Nátlak na nákup produktů nebo služeb, které nemusí být tak kvalitní nebo potřebné.
- ☐ Přílišná idealizace jejich životního stylu, která může vést k nespokojenosti se sebou samým.
- ☐ Ztráta času nebo soustředění na důležitější věci, jako je škola nebo rodina.
- ☐ Žádná rizika tam nevidím.

37. Jaké osobní údaje sdílíš na sociálních sítích/internetu? *

Vyber jednu nebo více odpovědí

Zaškrtněte všechny platné možnosti.

- ☐ Jméno a příjmení
- ☐ Datum narození
- ☐ Osobní fotografie
- ☐ Telefonní číslo
- ☐ E-mailovou adresu
- ☐ Adresu bydliště
- ☐ Aktuální polohu
- ☐ Bankovní údaje (číslo účtu nebo karty)
- ☐ PIN od bankovní karty
- ☐ Název a adresu školy, kam chodíš

38. Jak reaguješ, když dostaneš zprávu od neznámého člověka na sociálních sítích? *

Označte jen jednu elipsu.

- ☐ V klidu odpovím, pokud je zpráva zdvořilá a zajímavá – odpovím se zájmem.
- ☐ Odpovím, ale velmi opatrně a s rezervou.
- ☐ Ignoruji ji, pokud je od úplně cizí osoby.
- ☐ Okamžitě zablokuji osobu, která mi napsala.
- ☐ Nikdy jsem nedostal/a

39. Zveřejňuješ na sociálních sítích něco, co by mohlo ovlivnit tvoje soukromí v budoucnu? (místo, kde se nacházíš, osobní údaje, fotografie atd.) *

Označte jen jednu elipsu.

- ☐ Ano, sdílím osobní věci, protože mi to nevadí
- ☐ Občas, ale většinou se snažím být opatrný/á
- ☐ Ne, nikdy - dávám si pozor, co sdílím
- ☐ Nezveřejňuji nic osobního, co by mohlo mít dlouhodobý dopad

40. Přijímáš žádosti o přátelství nebo sledování od lidí, které osobně neznáš? *

Označte jen jednu elipsu.

- ☐ Ano, vždy
- ☐ Ano, pokud mají společné přátele
- ☐ Nikdy, přijímám pouze žádosti od lidí, které znám osobně
- ☐ Nemám sociální sítě

41. Co děláš pro to, aby ses těmto všem rizikům, která byly zmíněny v dotazníku, vyhnul/la? *

Vyber jednu nebo více odpovědí

Zaškrtněte všechny platné možnosti.

- ☐ Omezuji přístup k některým webům nebo aplikacím.
- ☐ Hlídám si svůj pohyb na internetu.
- ☐ Sdílím obavy s kamarády.
- ☐ Ignoruji všechny rizika (nevšímám si toho).
- ☐ Neotevírám odkazy od neznámých osob.
- ☐ Ověřuji si informace.
- ☐ Nestahuji neověřený obsah.
- ☐ Používám silná hesla.
- ☐ Sleduji, co sdílím online.
- ☐ Používám antivirový program.
- ☐ Blokuji nevhodné uživatele.
- ☐ Sdílím obavy s rodiči.
- ☐ Zajímám se o to, komu svěřuji své osobní údaje.
- ☐ Jiné: _____

42. Kde nejčastěji získáváš informace o digitální bezpečnosti? *

Vyber jednu nebo více odpovědí

Zaškrtněte všechny platné možnosti.

- ☐ Ve škole
- ☐ Od rodičů
- ☐ Od kamarádů
- ☐ Na internetu (např. videa, články)
- ☐ Jiné: _____

43. Cítíš, že jsi dostatečně vzdělaný/á v bezpečnosti v digitálním světě? *

Označte jen jednu elipsu.

- ☐ Ano, cítím se dobře informovaný/á.
- ☐ Částečně, mám nějaké znalosti, ale mohl/a bych se dozvědět víc.
- ☐ Ne, necítím se dostatečně informovaný/á.
- ☐ Nejsem si jistý/á, co všechno bych měl/a vědět.

44. Myslíš si, že tvoji rodiče nebo škola tě dostatečně informují o bezpečnosti na internetu? *

Označte jen jednu elipsu.

- ☐ Ano, poskytují mi dostatek informací.
- ☐ Ano, ale mohli by dělat více.
- ☐ Ne, nedostávám dostatek informací.
- ☐ Nevím, jaké informace bych měl/a dostávat.

KONEC DOTAZNÍKU

Děkuji Ti mockrát za vyplnění mého dotazníku a přeji Ti krásný den!

Obsah není vytvořen ani schválen Googlem.

Google Formuláře

PŘÍLOHA P 2: POLOŽKY V DOTAZNÍKU A VÝZKUMNÉ OTÁZKY

Hlavní výzkumná otázka	Jaký je pohled pubescentů na bezpečnost v digitálním světě?
Dílčí výzkumná otázka č. 1	Jaké typy digitálních rizik jsou pubescentům nejvíce známé?
Položka v dotazníku	3. Jaké typy digitálních rizik znáš?
	4. Kde jsi se o těchto rizicích dozvěděl/la?
Dílčí výzkumná otázka č. 2	Jaké jsou zkušenosti pubescentů s digitálními riziky při užívání online prostředí?
Položka v dotazníku	5. Chováš se na internetu bezpečně?
	7. Je podle tebe komunikace na internetu s lidmi, které neznáš, bezpečná?
	8. Komunikuješ na internetu s lidmi, které neznáš? (např. na sociálních sítích, při hraní her)
	9. Pokud ano, na jakých platformách s nimi komunikuješ?
	10. Setkal/a jsi se někdy s někým v online prostoru, kdo ti psal hodně osobní zprávy?
	11. Vyžadoval od tebe někdy někdo v online prostoru hodně osobní informace?
	12. Navrhl ti někdy člověk, kterého neznáš osobně, přes internet osobní schůzku?
	13. Napsal ti někdy někdo cizí na internetu podobnou zprávu? <i>„neříkej to rodičům, nepochopí to“ nebo „pokud jim to prozradíš, budeš mít problémy“</i>
	14. Nabízel ti někdo něco (peníze, nový telefon, oblečení, novou počítačovou hru) za to, že mu pošleš například své telefonní číslo, adresu bydliště nebo jiné podobné informace?
	16. Přišel ti někdy e-mail, který se ti zdál podezřelý? (byl od cizí osoby, zvláštní text, obsahoval odkaz)
	18. Klikl/a jsi někdy na odkaz, který ti přišel od kohokoliv, přitom jsi nevěděl/a, co se v odkaze nachází?

	19. Podařilo se ti někdy omylem stáhnout nějaký druh malwaru? (např. virus, trojský kůň, adware atd.)
	21. Viděl/a jsi nějaké nenávistné komentáře například pod příspěvky na sociálních sítích?
	22. Přišel ti někdy nenávistný komentář pod tvůj příspěvek? (fotka či video na sociálních sítích)
	23. Napsal/a jsi ty někdy takový komentář?
	24. Jak reaguješ na nenávistné komentáře, které vidíš pod příspěvky na sociálních sítích?
	26. Byla ti někdy zaslána pornografická fotografi e nebo video? (tzn. fotka či video, kde se nachází nahota)
	28. Poslal/a jsi někdy sám/sama fotku či video sebe, kde se nachází nahota? (nejen sebe)
	29. Měl/a jsi někdy pocit, že ti někdo neustále psal, komentoval tvoje příspěvky nebo se o tebe zajímal víc, než bylo ti příjemné?
	31. Dostal/a jsi někdy zprávu, která obsahovala informaci, o které jsi později zjistil/a, že byla nepravdivá?
	33. Sdílel/a jsi někdy online informaci, u které jsi později zjistil/a, že byla nepravdivá?
	34. Důvěřuješ informacím, které sdílí tví oblíbení YouTubeři/influenceri/streameri?
	35. Jaký si myslíš, že mají na tebe vliv osoby na internetu (influenceri, YouTubeři, streameri)?
	36. Jaká rizika podle tebe mohou být spojena s tím, že lidé sledují tyto osoby?
	37. Jaké osobní údaje sdílíš na sociálních sítích/internetu?
Dílčí výzkumná otázka č. 3	Jaké jsou pocity pubescentů při setkání s těmito riziky?
Položka v dotazníku	6. Cítíš se na internetu v bezpečí?
	15. Jak jsi se cítil/la, když jsi dostal/a nabídku, ve které ti osoba nabízela dárky výměnou za osobní informace?
	17. Jak se cítíš, když obdržíš podezřelý e-mail?

	20. Jak jsi se cítil/a, když jsi zjistil/a, že máš v počítači malware? (např. virus, trojský kůň, adware atd.)
	25. Jak se cítíš, když tě někdo na internetu uráží nebo zesměšňuje?
	27. Jak se cítíš po setkání s pornografickým obsahem, kterému ses nechtěně vystavil/a?
	30. Jak ses cítil/la, když ti někdo psal nebo tě kontroloval víc, než bylo pro tebe příjemné?
	32. Jak ses cítil/la, když jsi zjistil/a, že informace, kterou jsi dostal/anebo sdílel/a, byla nepravdivá?
Dílčí výzkumná otázka č. 4	Jaké strategie užívají pubescenti v prevenci rizik spojených s používáním digitálních technologií?
Položka v dotazníku	38. Jak reaguješ, když dostaneš zprávu od neznámého člověka na sociálních sítích?
	39. Zveřejňuješ na sociálních sítích něco, co by mohlo ovlivnit tvoje soukromí v budoucnu? (místo, kde se nacházíš, osobní údaje, fotografie atd.)
	40. Přijímáš žádosti o přátelství nebo sledování od lidí, které osobně neznáš?
	41. Co děláš pro to, aby ses těmto všem rizikům, která byly zmíněny v dotazníku, vyhnul/la?
	42. Kde nejčastěji získáváš informace o digitální bezpečnosti?
	43. Cítíš, že jsi dostatečně vzdělaný/á v bezpečnosti v digitálním světě?
	44. Myslíš si, že tvoji rodiče nebo škola tě dostatečně informují o bezpečnosti na internetu?