POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

Katedra bezpečnostních studií

Bezpečnostní rizika na sociálních sítích

Bakalářská práce

Examining the Dangers of Social Networking Sites

Bachelor thesis

VEDOUCÍ PRÁCE

Mgr. Josef Dubský

AUTOR PRÁCE

Tereza Kisby

PRAHA

2022

Čestné prohlášení:

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracovala samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpala, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 15. března 2022

……

Tereza KISBY

Poděkování

Poděkování bych chtěla věnovat zejména vedoucímu práce Mgr. Josefu Dubskému za věcné připomínky a odborné rady k jejímu zpracování. Velké díky dále patří účastníkům rozhovorů, vykonávaných pro účely praktické části této práce. V neposlední řadě bych chtěla poděkovat mé rodině a přátelům za jejich trpělivost.

Anotace

Tato bakalářská práce je orientována na problematiku bezpečnostních rizik, která hrozí v prostředí sociálních sítí. V teoretické části jsou definovány základní pojmy, které s daným tématem souvisí včetně nastínění problematiky závislosti na internetu, která je s tímto tématem neodmyslitelně spjata. Následuje úsek zabývající se druhy sociálních sítí a jejich drobnou charakteristikou. Největší část práce je zaměřena na popis vybraných rizik, kterými jsou kyberšikana, kybergrooming, sexting, phishing a hoaxy. Poslední části práce jsou věnovány právnímu zakotvení zmíněných útoků, jejich prevenci a budoucnosti těchto jevů. Rozhovory, které tvoří praktickou část následně slouží k doplnění teorie o zkušenosti nejen samotných obětí, ale i experta na danou problematiku.

klíčová slova

internet * sociální sítě * rizika * kyberšikana * Kybergrooming * sexting * phishing * hoaxy * prevence

Annotation

This Bachelor thesis deals with the risks associated with online social networking. The theoretical part comprises definitions of basic concepts related to this particular field and explores the issue of internet addiction, which inherently coincides with this topic. The paper then proceeds to briefly characterize different types of social networks. The most extensive part of the paper examines the specific risks involved in cyberbullying, cyber grooming and sexting, phishing and hoaxes. The final parts of the paper are concerned with legal protection against such attacks, their prevention and the future of these phenomena. The theoretical part is followed by the practical part. Here, the theory is complemented by accounts of experiences given in interviews both with victims themselves and with an expert in the field.

Keywords

Internet * social networks * risks * cyberbullying * cyber grooming * sexting * phishing * hoaxes * prevention

Obsah

Úvod

Rizika nejrůznějšího charakteru číhají na každém kroku. Ve většině případů se jedná o viditelná rizika, u kterých můžeme docela snadno vyhledat zdroj a eliminovat je. Velice aktuální téma dnešní doby je ale fenomén zvaný sociální sítě, kde se samozřejmě vyskytuje nepřeberné množství rizik, která jsou ale mnohdy skrytá a jejich negativní dopad se projeví až po čase, kdy už je těžké mu předejít nebo jej eliminovat. Sociální sítě mají samozřejmě spoustu výhod, kterými jsou snadná komunikace, seznamování se a udržování kontaktů nebo rychlá výměna informací a lidé je využívají zejména z tohoto důvodu. Spousta z nich si ale neuvědomuje výše zmíněná nebezpečí, která představují, a kterým se ve většině případů vystavují sami svým nezodpovědným chováním. Proto je důležité dbát na prevenci rizikového chování a informovanost o možných rizikách v tomto online prostředí hrozících. Tato práce je zaměřena právě na bezpečnostní rizika na sociálních sítích a slouží jako materiál pro šíření informovanosti o této problematice.

Práce je rozdělena na dvě části, tedy teoretickou a praktickou. Teoretická část se skládá z šesti kapitol, kdy v první kapitole jsou definovány základní pojmy nepopíratelně související s problematikou rizik na sociálních sítích a jsou uvedeny základní informace o nich. Jedná se o pojmy internet, kybernetická kriminalita, kybernetický útok a sociální sítě. Druhá kapitola je věnována základnímu dělení sociálních síti na domácí a zahraniční a jsou popsány jednotlivé nejpopulárnější druhy v obou těchto kategoriích. Nejvýznamnější kapitolu této části tvoří třetí kapitola, ve které jsou rozebrány útoky hrozící na sociálních sítích, jejichž projevy mohou být kvalifikovány jako trestné činy. Zahrnuta je do této kapitoly také podkapitola zabývající se situací na sociálních sítích v době pandemie COVID-19. Čtvrtá kapitola je soustředěna na právní zakotvení jednotlivých forem zmíněných útoků, kdy oporou pro zpracování je trestní zákoník. V páté kapitole je přiblíženo téma prevence – co si pod tímto pojmem představit, jaké druhy prevence známe a existence preventivních programů. Poslední kapitola je orientována na možný vývoj sociálních sítí do budoucna a je nastíněn názor odborníka na toto téma. Praktická část je tvořena třemi řízenými strukturovanými rozhovory – dva z nich s oběťmi kyberšikany a jeden s expertem na danou problematiku.

Cílem této práce je tedy pomocí deskriptivní metody přiblížit základní pojmy týkající se sociálních sítí, jejich druhy a zejména vymezit podstatu jednotlivých vybraných útoků a závadových jednání odehrávajících se na sociálních sítích, k čemuž je využita také metoda analyticko-syntetická. Rozhovory v praktické části jsou realizovány pomocí metody individuálního expertního dotazování, jejichž cílem je získání dat, jejichž komparací a analýzou jsou následně formulovány závěry se zaměřením na možnost prevence rizik na sociálních sítích. Zároveň má text celé práce sloužit jako nástroj pro verifikaci či falsifikaci následujících tři ad hoc stanovených hypotéz:

1. Situace týkající se útoků na sociálních sítích se výrazně zhoršila v době pandemie COVID-19.
2. Děti do patnácti let jsou nejnáchylnější k tomu stát se oběťmi útoků na sociálních sítích.
3. Ve věcech sociálních sítí můžeme blízkým osobám vždy důvěřovat.

Největší literární oporou pro zpracování této práce jsou knihy Bezpečně n@ internetu od autorů Martina Kožíška a Václava Píseckého a Internetová kriminalita páchaná na dětech od Lenky Hulanové. Čerpáno je ale také z dalších knih, právních předpisů a internetových zdrojů, a to jak českých, tak i cizojazyčných. Citace veškerých využitých zdrojů jsou konstruovány pomocí stránek citace.com.

I. TEORETICKÁ ČÁST

1 Základní pojmy

Tato kapitola je věnována čtyřem základním pojmům vztahujícím se k problematice rizik na sociálních sítích, a to zejména proto, aby bylo čtenářům usnadněno porozumění následujícího textu. Jedná se o pojmy internet a jeho odlišnosti od pojmu kyberprostor, dále kybernetická kriminalita a kybernetický útok a zakončena bude tato kapitola pojmem sociální sítě. Tyto pojmy jsou základem daného tématu práce a bez nich by nebyl její obsah úplný a dostatečně srozumitelný.

1.1 Internet

Internet, úzce spojen s pojmem kyberprostor, je dnes nedílnou součásti života každého z nás. Tento pojem si představíme, když se řekne práce, zábava, vzdělávání, nakupování a zejména komunikace a sociální interakce, které probíhají prostřednictvím počítače či jiného elektronického zařízení. Jedná se o slovo mezinárodně využívané, kterému by rozuměl snad i člověk z opačných koutů světa.

Z poloviny je to pojem latinského původu (inter – mezi) a z druhé poloviny anglického původu (net – síť). Využívání internetu mělo od jeho zveřejnění rapidní nárůst. *„Již čtyři roky po jeho otevření široké veřejnosti získal 50 milionů uživatelů. Pro srovnání, rádio získalo stejný počet uživatelů za 30 let a televize za 13 let.“* [1] Tomu, co to přesně internet je a jeho spojitostmi s kyberprostorem bude věnována následující podkapitola.

1.1.1 Internet a kyberprostor

Pojem internet a s ním spojený kyberprostor, jak již bylo zmíněno, se velkým dílem prolínají a ve většině případů se považují za totéž. Základní definicí, která pojímá ve své podstatě oba pojmy je definice ze Zákona o kybernetické bezpečnosti, která říká, že: *„kybernetickým prostorem se rozumí digitální prostředí umožňující*

[1] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9. s. 17.

vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“ [2]

Podle autora Jana Koloucha existují určité odlišnosti mezi internetem a kyberprostorem, a to zejména v tom, že internet dává jakýsi základ systému formujícího kyberprostor, který je ale, jak také uvádí, sám o sobě těžko vymezitelný.[3] Ve své knize CyberCrime předkládá následující pojetí internetu:

„Materiální podstatou internetu je jeho páteřní síť, která vede signál vzduchem, kabely, či jinými přenosovými médii. Technicky se jedná o celosvětovou distribuovanou počítačovou síť složenou z jednotlivých menších sítí, které jsou navzájem spojeny pomocí protokolů IP a tím je umožněna komunikace, přenos dat, informací a poskytování služeb mezi subjekty navzájem.“[4]

Co se týče kyberprostoru, dle téhož autora se jím rozumí: *„Virtuální realita, nemající ani konec ani začátek. Prostor kybernetických aktivit či prostor vytvořený informačními a komunikačními technologiemi, který vytváří virtuální svět jako paralelu prostoru reálnému.“*[5]

Je tedy jasné, že internet a kyberprostor mají mnoho společného, zejména to, že by jeden bez druhého neexistoval.

Pro upřesnění ještě uvedu definici, kterou ve své knize uvádí Lenka Hulanová, a která nám dává zcela jasný pohled na souvislosti mezi těmito pojmy: *„Kyberprostor je prostor, který se nám otevírá ve chvíli, kdy pomocí internetových sítí vstupujeme do on-line prostředí.“*[6]

Tímto jsou pojmy internet a kyberprostor jasně definovány a odlišeny a můžeme se posunout na další podkapitolu, která bude zaměřena na historii internetu.

---

[2] Viz § 2 Zákona č. 181/2014 Sb., *o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) v posledním znění*

[3] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 43.

[4] Tamtéž

[5] Tamtéž

[6] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9. s. 27.

1.1.2 Historie internetu

Ve světě v roce 2021 dosáhl počet připojených k internetu 4,9 miliard lidí, což jsou téměř dvě třetiny celkové světové populace.[7] Nebylo tomu tak ale vždycky. Poprvé se k internetu připojili ve Spojených státech amerických v roce 1969, a to díky státní agentuře ARPA (Advanced Research Project Agency – Agentura pro pokročilý výzkum), která v roce 1968 zveřejnila veřejnou zakázku vyzývající zejména vědce k předložení návrhů, jak zrealizovat výměnu zpráv či nejrůznějších sdělení mezi jednotlivými počítači. Na řešení přišel Joseph Carl Robnett Licklider s jeho týmem. Na principech, se kterými přišli, je založen internet i dnes. První primitivní předchůdce internetové sítě, která fungovala mezi čtyřmi americkými univerzitami a Bostonem, se nazývala Arpanet. Na začátku 70. let se tato síť rozšířila do mnoha univerzit a společností po celých spojených státech. Až teprve v roce 1973 se propojil s evropskými zeměmi, přesněji s Velkou Británií a Norskem. Současně s Arpanetem ale existovaly sítě například ve Francii nebo na Havaji, nebyly však navzájem slučitelné. Prvními, kdo dokázali sítě propojit, byli Bob Kahn a Vint Cerf, kterým se to podařilo díky protokolu TCP/IP (Transmission control protocol – Protokol řízení přenosu a Internet protocol – Internetový protokol). Česká republika se ale k internetu připojila až v roce 1992.[8] Od té doby je k internetu připojeno víc a víc lidí nejen v České republice, ale po celém světě. Údajům vztahujícím se konkrétně k využívání internetu v České republice bude věnována následující kapitola.

1.1.3 Statistická data týkající se využívání internetu v ČR

V dnešní době je internet využíván ve většině domácností. Osobně si nedovedu představit svět bez připojení k internetu a troufám si říci, že téměř nikdo to již nedovede. Výjimky samozřejmě existují, jimi se ale tato práce nezabývá.

Česká republika je k internetu připojena, jak již bylo zmíněno, od roku 1992 a podle Českého statistického úřadu se počet domácností připojených k internetu

[7] JOHNSON, Joseph. Internet usage worldwide – statistics & facts. *Statista* [online]. 25.1.2022 [cit. 2022-03-05]. Dostupné z: https://www.statista.com/topics/1145/internet-usage-worldwide/#topicHeader__wrapper

[8] OTEVŘENÁ VĚDA, Odborný garant dílu - doc. Ing. Pavel Peterka, Ph.D. NEZkreslená věda: pátá série vzdělávacího cyklu Akademie věd České republiky.: JAK FUNGUJE INTERNET – NEZkreslená věda V. *YouTube* [online]. 4. 5. 2020, 9:48 minut. [cit. 2021-12-15]. Dostupné z: https://www.youtube.com/watch?v=L05HGoaDkRo&ab_channel=Otev%C5%99en%C3%A1v%C4%9Bda

neustále zvyšuje. Například od roku 2010 se tento počet zvýšil z 56 % na celých 83 % v roce 2021.[9] Exponenciální růst těchto údajů nám dává jasnou známku toho, že domácnosti jsou čím dál více závislé na internetovém připojení ať už dobrovolně nebo je k tomu donutí práce či jiné nezbytné aktivity, které se dají vykonat dnes již pouze prostřednictvím internetu. Jedná se zejména o domácnosti, ve kterých je alespoň jedno dítě, neboť studium jakékoli školy je dnes podmíněno dostupností internetového připojení a vlastnictvím určitého zařízení, přes které se lze k internetu připojit, ať už se jedná o mobilní telefon, počítač či tablet. Vyplývá to i z údajů Českého statistického úřadu, který uvádí, že oproti domácnostem bez dětí, kterých je připojeno 77,3 %, domácností připojených k internetu s alespoň jedním dítětem je 99,3 %.[10] V dnešní době je jistě nezbytností mít v domácnosti internet, s jeho využíváním se to ale nesmí přehánět, neboť nadměrné užívání internetu může vést k závislosti na něm. O tomto nešvaru bude pojednávat následující kapitola.

1.1.4 Závislost na internetu

Závislost na internetu, problém 21. století, který však ne všichni dokážou rozeznat. Ne všichni jsou si totiž vědomi reálné existence této obtíže a tím pádem nejsou schopni ji včas odkrýt a řešit. Každý je seznámen s hrozbou závislosti na alkoholu, cigaretách, automatech či na práci a je schopen ji v určité fázi podle daných znaků poznat. Kdo však dokáže říci, kdy je člověk závislí na internetu? Nejen proto, aby bylo na tuto otázku odpovězeno, ale i z důvodu toho, že závislí na internetu jsou náchylnější k tomu, stát se oběťmi útoků na sociálních sítích[11], je do této práce zahrnuta právě tato kapitola.

Definovat problematiku závislosti na internetu je relativně obtížné. V dnešní době je za závislost na internetu považována spíše závislost na jednotlivých aplikacích a službách, které internet nabízí. „*Jedná se o poruchy, související s využíváním*

[9] Využívání informačních a komunikačních technologií v domácnostech a mezi osobami - 2021: Počítače a internet v domácnostech - Tab. 1.4 Domácnosti v ČR s internetem – vývoj v čase. *Český statistický úřad* [online]. 23.11.2021 [cit. 2021-12-15]. Dostupné z: https://www.czso.cz/csu/czso/1-pocitace-a-internet-v-domacnostech-f1de7iri8s
[10] Tamtéž
[11] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9. s. 48.

internetu, mezi které patří zejména závislost na online počítačových hrách, závislost na kybersexu, online gambling a závislost na online sociálních sítích.“[12]

I přes to existuje šest kritérií, podle kterých lze identifikovat závislost na internetu. Mark Griffiths je definoval následovně:

1. „Význačnost“ – pro uživatele je daná činnost nejpodstatnější a na úkor toho zanedbává vlastní, mnohem důležitější životní nezbytnosti.

2. „Změny nálad“ – v důsledku užívání internetu.

3. „Abstinenční příznaky“ – pokud nemá jedinec přístup k aktivitě, na které je závislý.

4. „Tolerance“ – závislí potřebuje stále víc a víc dané aktivity.

5. „Konflikt“ – jedinec tráví čím dál více času na internetu, tím pádem musí obětovat jiné činnosti, kterým se dříve věnoval a rád. Tím může vzniknout například mezilidský konflikt s přáteli nebo rodinou.

6. „Relaps“ – závislí si sice přizná, že tráví moc času na internetu a snaží se to omezit. Po nějaké době se však vrací k původnímu nežádoucímu scénáři.[13]

Lukas Blinka a David Šmahel vytvořili škálu, která obsahuje šest výše zmíněných dimenzí, pro měření závislosti na internetu. Ta však neslouží pro přesnou klinickou diagnózu, pouze orientačně. Škála obsahuje deset otázek s možnostmi odpovědí: *„nikdy – zřídka – často – velmi často a za závislého lze považovat toho, kdo odpoví alespoň na jednu položku v každé z dimenzí často nebo velmi často*:

- *dimenze význačnosti:*
  1. Zanedbáváte někdy své potřeby (např. jídlo či spánek) kvůli internetu?
  2. Představujete si, že jste na internetu, i když na něm právě nejste?
  3. Stává se vám, že jste na internetu byl/a výrazně déle, než jste původně zamýšlel/a?
- *dimenze tolerance:*
  4. Máte pocit, že na internetu trávíte stále více a více času?
  5. Přistihnete se, že brouzdáte po internetu, i když vás to už vlastně nebaví?

[12] BLINKA, Lukáš. *Online závislosti: jednání jako droga? online hry, sex a sociální sítě: diagnostika závislosti na internetu: prevence a léčba*. Praha: Grada, 2015. Psyché (Grada). ISBN 978-80-247-5311-9. s. 33.
[13] ŠEVČÍKOVÁ, Anna. *Děti a dospívající online: vybraná rizika používání internetu*. Praha: Grada, 2014. Psyché (Grada). ISBN 978-80-247-5010-1. s. 44.

- *Dimenze změn nálad:*

  6. Cítíte se veselejší a šťastnější, když se dostanete konečně na internet?
- *Dimenze abstinenčních příznaků:*

  7. Cítíte se neklidná/ý, mrzutá/ý nebo podrážděná/ý, když nemůžete být online?
- *Dimenze relapsu:*

  8. Pokusil/a jste se někdy neúspěšně omezit čas, který jste na internetu?
- *Dimenze konfliktu:*

  9. Hádáte se někdy se svými blízkými (rodina, přátelé, partner/ka) kvůli času, který trávíte na internetu?

  10. Strádá vaše rodina, přátelé, práce, či zájmy kvůli času, který trávíte na internetu?"[14]

V případě, že jedinci (byť jen orientačně) vyjde, že je s největší pravděpodobností závislý na internetu, měl by to, stejně jako každou jinou závislost, řešit. Podle Kimberly Youngové je nejdůležitější *„práce s motivací, změna životního stylu, využívání vlivu širšího okolí, rozpoznávání spouštěčů a vyhýbání se jim nebo jejich lepší zvládání, prohlubování sebeuvědomění, udržování dobrého stavu a prevence relapsů. Závislost na internetu však může být pro jedince úniková cesta od jiných duševních problémů, které se, v případě že se to potvrdí, musí léčit primárně."*[15]

Internet je tedy dnes nepostradatelnou záležitostí každodenního života lidí po celém světě. Se všemi možnostmi, které nám ale nabízí s sebou přináší i jisté problémy nejen v podobě závislosti, ale i například v podobě kriminality, která je dnes na internetu hojně vyskytována v nejrůznějších podobách. Tato práce je zaměřena na útoky realizované prostřednictvím internetu, konkrétně sociálních sítí, jejichž formy mohou být klasifikovány jako trestné činy, proto následující podkapitoly budou věnovány pojmům jako je kybernetická kriminalita a kybernetický útok.

[14] ŠEVČÍKOVÁ, Anna. *Děti a dospívající online: vybraná rizika používání internetu*. Praha: Grada, 2014. Psyché (Grada). ISBN 978-80-247-5010-1. s. 46-47.
[15] NEŠPOR, Karel. *Návykové chování a závislost: současné poznatky a perspektivy léčby*. 5., rozšířené vydání. Praha: Portál, 2018. ISBN 978-80-262-1357-4. s. 48.

1.2 Kybernetická kriminalita

Základní definicí kybernetické kriminality je ta, kterou využívá Policie ČR. Ta ji vymezuje jako „*trestnou činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí. Samotná oblast informačních a komunikačních technologií je buď předmětem útoku, nebo je páchána trestná činnost za výrazného využití informačních a komunikačních technologií jakožto významného prostředku k jejímu páchání.*“[16]

Podle Lenky Hulanové *„internetová kriminalita obecně zahrnuje takovou trestnou činnost, kde je síťové připojení nástrojem, cílem nebo místem spáchání trestného činu.“*[17] Kybernetická trestná činnost v sobě pojímá nepřeberné množství nezákonných činností, jako například vydírání, podvody, krádeže, ale i kriminalitu páchanou na dětech. Tato autorka ve své knize také uvádí obecné rozdělení těchto aktivit do tří kategorií:

1. *„trestné činy, které se zaměřují na počítačové sítě nebo zařízení přímo“*
   příklady:
   - *malware*
   - *počítačové viry*
2. *„trestné činy, které jsou usnadněny pomocí počítačových sítí nebo zařízení“*
   příklady:
   - *kyberstalking*
   - *krádeže identity a podvody s tímto spojené*
   - *phishing, pharming*
3. *„internetová kriminalita páchaná na dětech“*
   příklady:
   - *kyberšikana*
   - *Kybergrooming*
   - *on-line dětská pornografie.“*[18]

[16] Kyberkriminalita. *Policie České republiky* [online]. [cit. 2022-02-06]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx
[17] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9. s. 34.
[18] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9. s. 34.

1.3 Kybernetický útok

Co se týče kybernetického útoku Jan Kolouch ho definuje jako *„jakékoli protiprávní jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby. Tato jednání nemusí mít vždy podobu trestného činu, podstatné je, že narušují běžný způsob života poškozeného. Kybernetický útok může být dokonán, stejně jako může být ve stádiu přípravy či pokusu. Propojení kybernetického trestného činu a kybernetického útoku je v tom, že ne každý kybernetický útok je trestný čin, ale kybernetický trestný čin musí být vždy kybernetickým útokem.“*[19]

Jak již bylo zmíněno, jednou ze služeb, které umožňují pachatelům realizovat kybernetické útoky, a tak páchat i kybernetickou trestnou činnost, jsou sociální sítě, které budou předmětem následující podkapitoly.

1.4 Sociální sítě

Dalším významným termínem, který je třeba specifikovat, než se dostaneme do samého jádra této práce je sociální síť. Sociální sítě jsou fenoménem dnešní doby, zejména u mladé generace a jedná se o nejvyužívanější služby na internetu, kde uživatelé sdílejí své fotografie, videa, hudbu nebo nabídky například služeb, práce nebo bydlení.

Předchůdcem dnešních sociálních sítí byla síť nazývaná Sixdegrees.com z roku 1997. Tato síť jako první umožňovala registraci a kontakt mezi známými. V roce 2001 byla sice ukončena, ale dodnes je považována za projekt, který dal vzniknout myšlenkám vedoucím k vytvoření sociálních sítí, jak je známe dnes.[20]

Definice sociálních sítí byla pro účely této práce vybrána z knihy Bezpečně n@ internetu, kde autoři Martin Kožíšek a Václav Písecký uvádí, že: *„Sociální síť je internetová služba, která umožňuje svým členům vytvářet veřejné, uzavřené nebo i firemní profily, prezentace, diskuzní fóra, a nabízí prostor pro sdílení fotografií, videí, obsahu a dalších aktivit.“* [21]

---

[19] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 55.
[20] Sociální sítě: Co je sociální síť. *Nebojte se Internetu* [online]. cz.nic [cit. 2022-02-11]. Dostupné z: https://www.nebojteseinternetu.cz/page/3396/socialni-site/
[21] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3. s. 24.

Mojmír Král ve své knize uvádí, že *„pod spojením sociální sítě si lze představit virtuální propojení lidí a skupin, mezi nimiž lze sdílet informace, a že právě toto sdílení je podstatou sociálních sítí, jen každá sociální síť poskytuje do určité míry jiné možnosti sdílení informací. Za sdílení informací lze podle tohoto autora považovat psaní vlastních příspěvků, hodnocení a komentování příspěvků ostatních uživatelů, vkládání a hodnocení fotografií, zapojení se do diskusních skupin, doporučení určitého obsahu ostatním uživatelům.“* [22]

Sociální sítě mají své rysy, kterými se vyznačují. Jsou jimi:

- *„Vytváření komunit“* – Na sociálních sítích je možné vytvářet kolektivy lidí se stejnými zájmy, náboženskými vyznáními nebo názory. Spojovat se a sdílet mezi sebou například své nadšení pro určitý druh hudby, sportu nebo filmů zde mohou lidé z celého světa.
- *„Založení profilu“* – Každý, kdo má zájem zapojit se do virtuálního světa pomocí sociálních sítí si musí na zvolené síti vytvořit svůj profil, a to zejména proto, aby byl dohledatelný jinými uživateli a mohl se s nimi spojovat.
- *„Interakce“* – Posledním znakem je interakce, což znamená, že uživatelé dané sociální sítě mohou vyjadřovat své postoje nebo pocity a myšlenky pomocí veřejných příspěvků a ostatní uživatelé na ně mohou reagovat.[23]

Co se týče kladů a záporů sociálních sítí, mají obojího nespočet. Klady jsou zejména snadná komunikace mezi lidmi, získávání informací a jejich rychlý přenos, vzdělávání, virtuální cestování a poznávání jiných zemí, nakupování ale také podpůrné skupiny nejrůznějších druhů. Lidé například vytvářejí skupiny, kam se mohou přidat uživatelé se stejnými zdravotními či psychickými problémy a dokážou si pomáhat a podporovat se navzájem. Mezi zápory patří především sociální nerovnováha, kdy uživatelé s oblibou sledují fotky a příspěvky známých, u nás především zahraničních, osobností a sami se s nimi srovnávají, považují je za dokonalé, i když realita je úplně odlišná. Zejména mladé dívky se často snaží dosáhnout vzhledu a postavy modelek prezentujících se na sociálních sítích, což v nejhorších případech vede ke zdravotním problémům, a to především

[22] KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: Grada Publishing, 2015. Průvodce (Grada). ISBN 978-80-247-5453-6. s. 171.
[23] Sociální sítě: Znaky sociálních sítí. *Nebojte se Internetu* [online]. cz.nic [cit. 2022-02-11]. Dostupné z: https://www.nebojteseinternetu.cz/page/3396/socialni-site/

psychického rázu. Na mysli mám hlavně anorexii a bulimii. Z toho důvodu je nutná osvěta mladé generace o tom, že ne vše, co vidí na sociálních sítích je pravda. Co se týče zdravotních problémů je se sociálními sítěmi spojen ještě například nedostatek spánku, který je způsobený narušením spánkového cyklu. Dalším záporem sociálních sítí je odvádění pozornosti, a to zásadně ve chvíli, kdy musíme plnit úkoly jakéhokoli charakteru. Za negativní se dále považuje fakt, že v dnešní době již vymírá tzv. off-line komunikace a lidé raději komunikují a tráví čas online, než aby se scházeli face-to-face.[24] Dalšími negativními jevy jsou útoky realizované skrz sociální sítě, kterým bude věnována samostatná kapitola. Nyní však následuje kapitola, která nám umožní představit si, kolika lidí v České republice se týkají problémy a nebezpečí, na které je tato práce zaměřena.

1.4.1 Statistická data týkající se využívání sociálních sítí v ČR

V této kapitole bude opět čerpáno z údajů Českého statistického úřadu pro rok 2021. Česká republika má již více než 10,5 milionů obyvatel a Český statistický úřad uvádí následující data. Ve věku od 16 do 74 let využívá sociální sítě 61,5 % obyvatel České republiky. Od roku 2010 se tento počet zvýšil, a to z pouhých 10,1 %. Zde opět vidíme, stejně jako u využívání internetu, že počet uživatelů roste a s největší pravděpodobností poroste i nadále. Obecně lze říci, že ženy využívají sociální sítě procentuálně o něco více než muži. Konkrétně u žen starších 16 let mluvíme o 58 %, u mužů o 54,4 %. Co se týče věkových skupin, největší zastoupení na sociálních sítích má skupina 16-24 let, přesně 95,4 %. Na druhém místě, jak by se dalo i logicky odvodit, je věková kategorie 25-34 let, a to konkrétně 92,9 %. Nejnižší procentuální zastoupení na sociálních sítích má věková skupina 65+ a to pouhých 10,6 %. V roce 2010, pro porovnání, to bylo ale pouhých 0,4 %. Ráda bych také zmínila procentuální podíl občanů z pohledu ekonomické aktivity, kde jasně vedou studenti s celými 96,6 %. „*Procentuální vymezení je podíl z celkového počtu osob v dané socio-demografické skupině.“*[25]

[24] Bára. Sociální sítě – nevýhody. *JA IT* [online]. 27.2.2022 [cit. 2022-03-05]. Dostupné z: https://www.jait.cz/post/socialni-site-nevyhody

[25] Využívání informačních a komunikačních technologií v domácnostech a mezi osobami - 2021: 7. Sociální sítě - Tab. 7.2 Osoby v ČR používající sociální sítě – vývoj v čase. *Český statistický úřad* [online]. 23.11.2021 [cit. 2022-01-02]. Dostupné z: https://www.czso.cz/csu/czso/7-socialnisite

Co se týče celkového postavení České republiky v Evropě ve využívání sociálních sítí pro měsíc leden 2021, nacházela se v té době na patnáctém místě s 7,39 miliony uživatelů. První místo zaujalo Rusko, které mělo v daném měsíci 99 milionů uživatelů sociálních sítí. Na posledním místě, tedy padesátém, se objevilo Monaco s 0,01 miliony uživatelů ve sledovaném měsíci.[26]

Pro porovnání: *„Počet lidí využívajících sociální sítě celosvětově pro rok 2021 byl více než 3,96 miliardy, tedy 50,64% populace, přičemž průměrný uživatel má 8,8 účtů na různých sociálních sítích.“*[27] Nejvyužívanějším sociálním sítím, jak českým, tak i zahraničním, bude věnována následující kapitola.

[26] Number of monthly active mobile social media users in Europe as of January 2021, by country. *Statista* [online]. Statista Research Department, 28.1.2022 [cit. 2022-02-20]. Dostupné z: https://www.statista.com/statistics/299496/active-mobile-social-media-users-in-european-countries/

[27] Statistiky využití sociálních sítí: Kolik lidí používá sociální média v roce 2021?: KOLIK LIDÍ POUŽÍVÁ SOCIÁLNÍ SÍTĚ?. *Ler.studio* [online]. 22.6.2021 [cit. 2022-01-23]. Dostupné z: https://lerstudio.cz/statistiky-vyuziti-socialnich-siti-kolik-lidi-pouziva-socialni-media-v-roce-2021

2 Druhy sociálních sítí a jejich charakteristika

V současnosti existuje mnoho sociálních sítí nehledě na jejich využívanost a smysluplnost. Některé sociální sítě můžeme označit za více užitečné, a to zejména ty, které slouží k šíření pracovních nabídek či udržování kontaktů s přáteli a některé jsou spíše pro zábavu.

Základní dělení sociálních sítí, jak již bylo naznačeno, je na profesní a osobní. Osobní sociální sítě slouží ke komunikaci mezi jednotlivci, tedy mezi každým jedním registrovaným uživatelem a jsou jimi například Instagram, Ask.fm, Facebook nebo Tinder. Profesní sociální sítě jsou naopak určeny ke komunikaci organizací či pracovišť za účelem shánění zejména zaměstnanců. Takovou sociální sítí je například LinkedIn.[28]

Dalším významným dělením je na české a zahraniční sociální sítě.

2.1 České sociální sítě

I přes to, že jsou české sociální sítě na ústupu vzhledem k razanci a rozpětí těch zahraničních, existuje pár v České republice stále oblíbených. Jedná se o sociální sítě sloužící k seznamování a hledání si ideálního partnera či partnerky.

- Líbímseti.cz

Líbímseti.cz je nejoblíbenější česká sociální síť, která je v provozu již od roku 2002. Její hlavní náplní je spojovat mezi sebou její uživatele, umožňovat jim například komunikaci nebo sdílení fotografií. Funguje tedy na principu seznamky a v současné době je na této síti zaregistrovaných přes 1 400 000 uživatelů.[29]

- Seznamka.cz

Seznamka.cz se řadí mezi další české seznamky, na kterých je možné navázat partnerský vztah, ale i jenom nezávazný flirt, fungující od roku 1998. Po registraci má uživatel možnost zvolit si z 12 nabízených kategorií, podle jeho preferencí.[30]

[28] Sociální sítě: Dělení sociálních sítí. *Nebojte se Internetu* [online]. cz.nic [cit. 2022-02-11]. Dostupné z: https://www.nebojteseinternetu.cz/page/3396/socialni-site/
[29] Reklama. *Líbím se ti* [online]. [cit. 2022-01-23]. Dostupné z: http://napoveda.libimseti.cz/reklama/
[30] Přehled seznamovacích kategorií. *Seznamka.cz* [online]. [cit. 2022-01-23]. Dostupné z: https://www.seznamka.cz/inzeraty/kategorie.aspx

Dalšími Českými sociálními sítěmi jsou například XChat.cz a Štěstí.cz, které také slouží k seznamování se.

2.2 Zahraniční sociální sítě

Zahraničních sociálních sítí máme nepřeberné množství a nejrůznější druhy. V České republice v roce 2021 patřily mezi nejpopulárnější Snapchat, Facebook, Instagram, Twitter a LinkedIn.[31] Mimo ty budou v této kapitole zmíněny i další známé světové sociální sítě.

- Snapchat

Snapchat je sociální síť, která je v provozu od roku 2011 a je určena ke sdílení fotografií či videí s konkrétními uživateli, které po pár vteřinách zmizí. K fotografiím se dají připisovat krátké zprávy či komentáře.

- Facebook

Facebook patří mezi nejoblíbenější sociální sítě dnešní doby a má 2,7 miliard aktivních uživatelů měsíčně.[32] Facebook byl spuštěn pro širokou veřejnost v roce 2006 a jeho zakladatelem je Mark Zuckerberg. Slouží zejména ke komunikaci mezi přáteli, ke sdílení názorů, myšlenek, informací, fotografií, ale i k šíření nabídek od pracovních, přes nabídky bydlení a spolubydlení až po prodej movitostí i nemovitostí.

- Instagram

Instagram je další velmi populární sociální síť, která byla spuštěna v roce 2010 a o deset let později, tedy v roce 2020, měla již 1 miliardu uživatelů.[33] Prostřednictvím této sítě mají uživatelé možnost sdílet fotografie či videa a vzájemně je hodnotit. Zároveň spolu mohou skrz tuto sociální síť komunikovat i

[31] Most popular social media platforms in the Czech Republic in 2021, by posting frequency. *Statista* [online]. Statista Research Department, 11.1.2022 [cit. 2022-02-20]. Dostupné z: https://www.statista.com/statistics/1281528/czechia-social-media-platforms-by-posting-frequency/

[32] Statistiky využití sociálních sítí: Kolik lidí používá sociální média v roce 2021?: STATISTIKY VYUŽITÍ SOCIÁLNÍCH MÉDIÍ. *Ler.studio* [online]. 22.6.2021 [cit. 2022-01-23]. Dostupné z: https://lerstudio.cz/statistiky-vyuziti-socialnich-siti-kolik-lidi-pouziva-socialni-media-v-roce-2021

[33] PAVLÍČEK, Michal. Instagram slaví 10 let. Aktivně ho používá miliarda uživatelů po celém světě. *Mobilnet* [online]. 6.10.2020 [cit. 2022-01-23]. Dostupné z: https://mobilenet.cz/clanky/instagram-slavi-10-let-aktivne-ho-pouziva-miliarda-uzivatelu-po-celem-svete-41860

nakupovat. Velmi oblíbená je možnost „sledovat“ známé osobnosti, ať už modelky, herce a herečky nebo zpěváky a zpěvačky, kteří zde sdílí svůj každodenní život.

- Twitter

Twitter je sociální síť, kde lidé mohou sdílet své názory, myšlenky, postoje, aktuální dění ze světa ale i obyčejné zprávy o tom, co ten daný den dělali nebo co si dali k obědu. Sdílet se dají i fotografie a je zde také možnost soukromých zpráv. Twitter byl spuštěn v roce 2006 a nyní má více než 386 milionů aktivních uživatelů.[34]

- LinkedIn

LinkedIn byl zveřejněn v roce 2002 a v současné době má více než 280 milionů uživatelů.[35] Tato sociální síť slouží k šíření pracovních nabídek. Je určena jak pro zaměstnavatele k hledání zaměstnanců, tak pro lidi, kteří hledají pracovní pozice.

Mezi další populární sociální sítě patří například TikTok, kde mají uživatelé možnost vytvářet a sdílet krátká videa na nejrůznější náměty, dávat jim tzv. „to se mi líbí“ a komentovat je a YouTube, jehož hlavním účelem je sdílení videí. Oblíbenými zahraničními seznamovacími sociálními sítěmi jsou zejména Badoo a Tinder.

Jak můžeme vidět rozpětí možností je opravdu veliké, z čehož můžeme soudit, že i rizika a útočníci číhající na těchto sítích budou ve velké míře zastoupeni. Rizika těchto sociální sítí jsou spatřována především v tom, že zejména mladé uživatelky, ale i uživatelé si často neuvědomují, kdo všechno se může skrývat za, na první pohled, věrohodně vypadajícím účtem a sdílejí své citlivé informace a fotografie, které mohou být později zneužity. Nebo si dokonce sjednávají osobní schůzky s neznámými uživateli, které v tom nejhorším případě končí fatálně. Jednotlivé druhy útoků budou přiblíženy v následující kapitole.

[34] 66 stručných faktů o marketingu sociálních sítí. *Mytimi* [online]. [cit. 2022-01-23]. Dostupné z: https://www.mytimi.cz/66-strucnych-faktu-o-marketingu/
[35] LINKEDIN: Sociální síť LinkedIn. *Sítě v hrsti* [online]. [cit. 2022-01-23]. Dostupné z: https://sitevhrsti.cz/socialni-site/linkedin/

3 Rizika užívání sociálních sítí a jejich charakteristika

Sociální sítě mají spoustu kladných, ale i záporných aspektů, jak již bylo zmíněno. Tato kapitola se bude zabývat konkrétními, a těmi největšími, zápory, kterými jsou útoky, jejichž projevy jsou klasifikovány jako trestné činy.

3.1 Kyberšikana

Kyberšikana je nežádoucí fenomén dnešní doby a jeden z nejčastějších útoků na internetu, který může mít závažný dopad na psychiku nejen oběti, ale i jejích blízkých a okolí. V současnosti se téměř veškeré aktivity přesouvají do on-line prostředí. Jedná se jak o činnosti pozitivního rázu, tak bohužel i o ty negativní. Jedním z nich je právě šikana. To však neznamená, že by klasická šikana přestala existovat, jen se částečně přenesla do kyberprostoru. V některých případech může docházet i ke kombinaci těchto dvou spolu souvisejících jevů.

Definic kyberšikany existuje nepřeberné množství, pro účely této práce byla vybrána ta z knihy Bezpečně n@ internetu od Martina Kožíška a Václava Píseckého, ve které uvádí, že: *„Kyberšikana je jakékoliv chování, jehož záměrem je vyvést z rovnováhy, ublížit, zastrašit nebo jinak ohrozit oběť za pomoci moderních informačních technologií.“*[36]

Abychom mohli hovořit o kyberšikaně v pravém slova smyslu, musí být naplněny základní prvky, kterými se vyznačuje. *„Jsou jimi opakovanost, odehrávání se prostřednictvím elektronických médií, záměrnost agresivního jednání ze strany útočníka, mocenská nerovnováha a oběť vnímá toto jednání jako nepříjemné a ubližující.“*[37]

Kyberšikana může mít nejrůznější podoby, od posmívání se a pomlouvání, přes zveřejňování nežádoucích fotografií a urážení až po vydírání. Některé formy se mohou zdát povrchní, ale i sebebanálněji vypadající projev kyberšikany může vést k vážným psychickým i zdravotním problémům. Alena Černá ve své knize Kyberšikana uvádí sedm možných projevů kyberšikany:

[36] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3. s. 62.
[37] ČERNÁ, Alena. *Kyberšikana: průvodce novým fenoménem*. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-247-4577-0. s. 21.

- ***„Vydávání se za někoho jiného a krádež hesla“***

Tato forma kyberšikany se vyznačuje tím, že se pachatel prohlašuje za oběť. Nejčastěji tím způsobem, že si vytvoří nový účet, kde využije informace a fotografie oběti a předstírá, že je ona. V horším případě pachatel odcizí heslo oběti a vydává se za ni skrz její účet. V obou případech může útočník napáchat značné škody.

- ***„Vyloučení a ostrakizace“***

Oběť této formy je vyřazena z určitého kolektivu lidí. V tomto případě se nejedná o typickou kyberšikanu, ale je sem řazena zejména z toho důvodu, že toto jednání může mít stejné dopady na oběť, jako jakýkoliv jiný projev kyberšikany.

- ***„Flaming“***

Flaming je druh hádky, která probíhá na internetu. Účastníci této hádky mohou být dva nebo více a při výměně názorů používají nadávky, sprostá slova, urážky a v některých případech i vyhrožování. Aby se jednalo o flaming jako formu kyberšikany, a ne pouze o ostrou výměnu názorů, musí být naplněny prvky uvedeny výše.

- ***„Kyberharašení a kyberstalking“***

Kyberharašení představuje přehnaně častou komunikaci ze strany agresora, tedy jednostrannou, která je pro oběť protivná a nežádoucí. Nejčastěji se jedná o zahlcování oběti zprávami. V případě kyberstalkingu se jedná o závažnější a nebezpečnější jednání, kdy útočník oběti vyhrožuje, zastrašuje ji či ji dokonce vydírá a ta má strach o svou bezpečnost.

- ***„Pomlouvání“***

K pomlouvání, někdy také nazývanému outingu, dochází v případě, že pachatel šíří lživá oznámení o oběti na internetu, které ji mají určitým způsobem uškodit. Tato forma kyberšikany má většinou dlouhodobé a závažné následky, a to z toho důvodu, že zveřejněné informace, byť nepravdivé, lze z internetu jen těžko odstranit.

- ***„Odhalení a podvádění“***

V tomto případě se jedná o publikování informací o oběti, které jsou důvěrné a intimní a byly určeny pouze agresorovi. Často se jedná o odhalení sexuální orientace a informací nebo i fotografií a videí podobného rázu.

- ***„Happy slapping***“

Happy slapping je název pro útok, který je ve své podstatě face-to-face, kdy jeden nebo více útočníků fyzicky napadne oběť. Jedná se ale o útok, který má daleko horší psychické následky u oběti než klasický fyzický útok, a to proto, že je útok natáčen na elektronické zařízení jednoho z útočníků a následně je celé video sdíleno na internetu, kde se, jako všechno, šíří nezastavitelnou rychlostí.[38]

Zdeněk Martínek mezi projevy řadí ještě například:

- ***„Bluejacking“***

Jedná se o šíření fotografií upravených přes nejrůznější aplikace k tomu sloužící, na kterých je oběť ztrapňována a znemožňována.

- ***„Internetové hlasování“***

V tomto případě se jedná o ankety, ve kterých, nejčastěji spolužáci, hlasují o méněcennosti a ubohosti oběti.

- ***„Internetové soutěžení“***

Oběť je vyzvána k tomu, aby se natočila při vykonávání uloženého úkolu, který je opět zesměšňující a někdy i nelibý až bolestivý, a aby video sdílela na sociálních sítích, jinak bude vyzyvateli pomlouvána.[39]

Prostředků umožňujících konání kyberšikany je mnoho. Alena Černá ve své knize Kyberšikana uvádí následující kanály umožňující šíření kyberšikany:

- *„Sociální sítě*
- *Online interaktivní hry*
- *Webové stránky*
- *Instant messaging a zprávy (SMS a MMS)*
- *Blogy*
- *Elektronická pošta (e-mail)*
- *Chatovací místnosti*
- *Internetové ankety, dotazníky“*[40]

[38] ČERNÁ, Alena. *Kyberšikana: průvodce novým fenoménem*. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-247-4577-0. s. 25-27.
[39] MARTÍNEK, Zdeněk. *Agresivita a kriminalita školní mládeže*. 2., aktualizované a rozšířené vydání. Praha: Grada, 2015. Pedagogika (Grada). ISBN 978-80-247-5309-6. s. 174-175.
[40] ČERNÁ, Alena. *Kyberšikana: průvodce novým fenoménem*. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-247-4577-0. s. 28.

Důležitá jsou také specifika kyberšikany, jelikož jsou zásadní pro její přesné vymezení. Lenka Hulanová ve své knize Internetová kriminalita páchaná na dětech uvádí specifika kyberšikany podle Vágnerové (2009) následovně:

- ***„Agresor“***

Na rozdíl od klasické šikany u kyberšikany, díky anonymnímu prostředí, nemusí být útočník fyzicky zdatný a silný. Může to být úplně kdokoliv, jelikož anonymita internetového prostředí dodává odvahu i těm, kteří by ji v realitě nenašli.

Autorka Maria Vašutová a kol. rozlišují několik druhů kyberagresorů podle Aleše Kavalíra:

1. „*Pomstychtivý andílek*“

   V tomto případě se jedná o jedince, který se nepovažuje za agresora. Často se stává, že byl sám obětí šikany nebo se mu jen nelíbí chování jeho oběti a mstí se nebo se snaží o její polepšení.

2. „*Bažící po moci*“

   Představitelé tohoto agresora touží po pozornosti. Snaží se dokázat vlastní hodnotu a cenu tím, že v druhých vzbuzují strach a vyhledávají k tomu velké publikum. V mnoha případech jsou sami oběťmi klasické šikany a v online prostředí si zvyšují sebevědomí a dodávají si sílu. Tento typ agresora je považován za velmi nebezpečný, jelikož si málokdy uvědomuje závažnost svého jednání.

3. „*Sprosté holky*“

   Těmito typy agresorů jsou nejčastěji dívky, které vytvoří skupinu a následně si vybírají oběť obvykle z řad jiných dívek. To ale neznamená, že by se obětí nemohl stát kluk. Tito agresoři se chtějí zviditelnit, proto vyhledávají pro svá jednání široké publikum a chtějí dosáhnout určité míry uznání.

4. „*neúmyslný kyberagresor*“

   Tito aktéři si v žádném případě neuvědomují, že konají kyberšikanu. Jedná se spíše o nepromyšlenou reakci například na určitou nepřátelskou konverzaci nebo na komentáře. Nedochází jim důsledky jejich jednání.[41]

[41] VAŠUTOVÁ, Maria. *Proměny šikany ve světě nových médií*. Ostrava: Filozofická fakulta Ostravské univerzity v Ostravě, 2010. ISBN 978-80-7368-858-5. s. 92-93.

- ***„Oběť“***

Obětí může být také kdokoliv, na internetu je každý zranitelný. Oběť může být cílená, kdy útočník oběť zná, ale i zcela náhodná, kdy si útočník vybírá až přímo na místě, tedy na internetu.

- ***„Absence fyzického násilí“***

Toto specifikum se vyskytuje pouze u kyberšikany, tím z ní dělá závažnější, než je klasická šikana, jelikož lze hůře rozeznat oběť.

- ***„Absence úniku“***

U kyberšikany téměř neexistuje možnost uniknout, útočník má možnost sledovat oběť, kontaktovat ji, a tedy útočit prakticky kdekoliv a kdykoliv a lze jen těžko odhadnout a předvídat tyto jeho kroky.

- ***„Opakování“***

Oběť má možnost, na rozdíl od klasické šikany, neustále si číst zprávy, výhružky, sledovat její zesměšňování na internetu, vidět svoje zveřejněné fotografie či videa a neustále se tedy vracet k projevům šikany a zažívat ji v podstatě pořád dokola.

- ***„Šíře publika“***

Kyberšikana, na rozdíl od klasické šikany, může být sledována stovkami, ale i tisícem diváků, a to po celém světě. Toto představuje obrovský psychický nátlak na oběť a většinou tomu bohužel nelze zabránit.[42]

Kyberšikana je opravdu závažný problém, ze kterého nevede téměř žádná cesta ven. Proto je třeba mít se na pozoru a být opatrný při pohybování se a komunikaci nejen na internetu. V knize Agresivita a kriminalita školní mládeže uvádí její autor Zdeněk Martínek následující „*základní pravidla při setkání s kyberšikanou:*

- *Okamžitě ukončit komunikaci.*
- *Nereagovat na žádné e-maily, SMS.*
- *Nic nemazat, vše archivovat – pokusit se zajistit důkazní materiál.*
- *Vše oznámit, v ideálním případě podat na Policii ČR trestní oznámení na neznámého pachatele*.“[43]

[42] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9. s. 48-49.
[43] MARTÍNEK, Zdeněk. *Agresivita a kriminalita školní mládeže*. 2., aktualizované a rozšířené vydání. Praha: Grada, 2015. Pedagogika (Grada). ISBN 978-80-247-5309-6. s. 179.

3.2 Kybergrooming

Kybergrooming je dalším negativním jevem vyskytujícím se na internetu. *„Jedná se o 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.“* [44]

Po zdařilém vylákání oběti na schůzku může dojít k *„sexuálnímu zneužití oběti, fyzickému násilí na oběti, zneužití oběti pro dětskou prostituci, k výrobě dětské pornografie apod.“*[45]

U kybergroomingu se můžeme setkat s typickými fázemi, kterými si útočník snaží získat důvěru oběti. Vedoucí projektu E-Bezpečí a Digidoupě doc. Mgr. Kamil Kopecký, Ph.D. charakterizuje pět etap získávání důvěry oběti:

1. „Vzbuzení důvěry a snaha izolovat oběť“

V této fázi se pachatel snaží o navázání blízkého kontaktu s obětí. Usiluje o získání důležitých informací a o vcítění se do její osoby. Chce být nápomocný a soucitný a ve své podstatě oběti naznačit, že je jediný, který jí rozumí a chápe. Na konec ji separuje od okolí a rodiny a tím si vytvoří ideální situaci pro uskutečnění útoku.

2. „Podplácení dárky či různými službami, budování kamarádského vztahu“

Vztah, který si groomer vytvořil v první fázi se v této etapě snaží podpořit a upevnit tím, že oběti kupuje nejrůznější hmotné dárky nebo služby.

3. „Vyvolání emoční závislosti oběti na osobě útočníka“

Po vytvoření důvěry se oběť útočníkovy svěří se svými největšími tajemstvími. Groomer se snaží být co největší oporou pro oběť, čímž si vytvoří unikátní vztah a oběť má zájem komunikovat pouze s ním, jelikož pachatel přesně ví, co kdy říct, ve všem s obětí souhlasí a ve všem ji vyhoví. Tím se vytvoří právě emoční závislost.

---

[44] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3. s. 72.

[45] Co je kybergrooming?. *E-Bezpečí* [online]. 14.1.2019 [cit. 2022-02-09]. Dostupné z: https://www.e-bezpeci.cz/index.php/71-trivium/1421-co-je-kybergrooming

4. „Osobní setkání“

Po vybudování si vzájemné vazby a závislosti oběti na pachateli ve většině případů přichází na řadu osobní kontakt. Často už k tomu ale dochází ve fázi podplácení službami, kdy groomer pozve oběť například do zoo nebo aquaparku.

5. „Sexuální obtěžování, zneužití dítěte“

Úplně na závěr, pokud oběť souhlasí se schůzkou, dochází k jejímu zneužití.[46]

Stejně jako u kyberšikany se rozlišují určité typy útočníků neboli kybergroomerů. Metodický materiál pro pedagogické pracovníky Národního centra bezpečnějšího internetu předkládá následující typologii pachatelů gybergroomingu:

- ***„Kvazivoyeur“***

Tento typ útočníka nemá za cíl vylákat oběť na osobní schůzku. Svou oběť pouze pozoruje skrz kameru, snaží se ji přimět k sexuálním projevům, čímž se uspokojuje.

- ***„Experimentátor“***

Typ experimentátor se celým procesem kybergroomingu baví. Využívá nejrůznější sociální sítě, často má vytvořených několik identit, a dokonce má ve většině případů i více obětí najednou.

- ***„Kriminálník“***

Kriminálník často nejedná za účelem uspokojení vlastních potřeb, ale pro účely spáchání určitého protiprávního jednání, ve většině případů pro výrobu pornografického materiálu.

- ***„Duševně nemocný“***

Už z názvu je patrné, že se jedná o jedince s určitou psychickou poruchou a jedná tedy na základě pudů, které jen v ojedinělých případech dokáže ovládat. Protiprávnost a následky jeho činů kvůli své nemoci nedomýšlí.[47]

---

[46] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9. s. 53.

[47] KYBERGROOMING A KYBERSTALKING: Metodický materiál pro pedagogické pracovníky. *Národní centrum bezpečnějšího internetu* [online]. PROJEKT ŠKOLA BEZPEČNĚ ONLINE, 2012 [cit. 2022-02-09]. Dostupné z: https://www.ncbi.cz/projekty/ukoncene-projekty/op-vk/opvk-skola-bezpecne-online.html

3.3 Sexting

Sexting je jedním z častých útoků na sociálních sítích. Jedná se o sdílení intimních zpráv, fotografií nebo videí se sexuální tématikou s druhou osobou. Běžně se tak děje mezi teenagery, kteří mají určitý typ vztahu, ale i u bezbranných dětí, od kterých jsou fotografie vylákány predátorem. V obou případech hrozí zneužití, ať už se jedná o vydírání oběti nebo zveřejnění z nutnosti pomsty partnerovi po rozchodu. Je třeba si uvědomit, že citlivý materiál vypuštěný do prostoru internetu nelze téměř v žádném případě kompletně odstranit, což je jedním z hlavních důvodů závažnosti tohoto problému, nehledě na to, že šíření sexuálního materiálu osob mladších osmnácti let je v České republice trestným činem.[48]

Existuje několik motivů pro uskutečňování sextingu:

„1. Sexting je vnímán jako součást romantických vztahů

2. Sexting funguje jako nástroj pro potlačení nudy

3. Sexting vzniká jako produkt sociálního tlaku

4. Sexting jako produkt konzumní společnosti, jako nástroj sebeprezentace

5. Sexting jako nástroj pomsty“ [49]

U tohoto útoku je zcela na konkrétní osobě, zda intimní fotografie pošle či nikoli. Proto je jediná možnost, jak se vyhnout danému riziku nešířit žádný materiál tohoto druhu.

Martin Kožíšek a Václav Písecký ve své knize Bezpečně n@ internetu popisují kroky, které je vhodné následovat v případě, že osoba již nějaký vlastní intimní materiál odeslala:

- *„Nezasílat žádné další fotografie, videa ani se neukazovat na kameře. Tím se osoba dostane do ještě větší pasti.*
- *Dát najevo nezájem a odpor k chování útočníka a přestat komunikovat.*
- *Zálohovat veškerou komunikaci a odebrat útočníka z přátel na dané sociální síti.*

[48] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3., s. 83-84.
[49] KOPECKÝ, Kamil a René SZOTKOWSKI. *E-Bezpečí: Sexting jako riziková forma komunikace (průvodce studiem)* [online]. Olomouc, 2018 [cit. 2022-02-09]. Dostupné z: https://www.pdf.upol.cz/fileadmin/userdata/PdF/VaV/2018/odborne_seminare/E-Bezpeci_-_Sexting_jako_rizikova_forma_komunikace.pdf

- *Bezodkladně se obrátit na Policii, případně kontaktovat specializované poradny.“*[50]

3.4 Phishing

Na začátek této podkapitoly, než bude definován samotný pojem phishing, bude vysvětleno, co je to sociální inženýrství, neboť to s tímto pojmem úzce souvisí.

Martin Kožíšek a Václav Písecký ve své knize Bezpečně n@ internetu uvádí následující definici sociálního inženýrství:

„Sociální inženýrství je způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace. Útoky obsahují prvky přesvědčování a manipulace a jsou vedeny buď náhodně, nebo cíleně na konkrétní osoby.“[51]

Phishing je slovo anglického původu v češtině znamenající „rybaření“ a jedná se v podstatě o útok, kdy útočníci využívají sociálního inženýrství k tomu, aby přesvědčili oběť k zaslání svých osobních, citlivých údajů, jako jsou nejčastěji přihlašovací údaje nebo údaje ke kreditní kartě.[52]

Následující příklad z praxe od odborníka Mgr. Marka Pačmaga, MBA, LL.M. jasně ukazuje propojení sociálního inženýrství a phishingu:

„Na Facebooku přijde uživateli zpráva, ve které stojí: „Pokud se chcete podívat na nahé fotografie spolužačky ze třídy, tak klikněte na odkaz níže.“ Samozřejmě jsou všichni ve většině případů na takové věci zvědaví, tak kliknou na odkaz. Ten je přesměruje na fiktivní stránku, která vypadá jako Facebooková, kde jsou vyzváni k tomu, aby se znovu přihlásili do svého účtu. V případě, že se přihlásí, dojde k sdělení přístupových údajů útočníkovi, který pak může s účtem nakládat podle svého.“

3.5 Hoaxy

Hoaxy jsou, obzvlášť v současné situaci, kdy nás sužuje pandemie COVID-19, velice časté téma nejrůznějších diskuzí. Hoax v překladu znamená poplašná

[50] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3. s. 89.
[51] Tamtéž. s. 37.
[52] Tamtéž. s. 123.

zpráva, což už samo o sobě naznačuje, že informace označené za hoaxy nejsou ve své celé podstatě pravdivé a, jak píšou na stránkách internetem bezpečně, jejich účelem je:

- *„Vyvolat strach*
- *Šířit falešnou radu*
- *Manipulovat s názory lidí*
- *Poškodit instituci, značku, firmu, výrobek*
- *Ohromit, zaujmout, přilákat pozornost*
- *Vystřelit si z důvěřivých uživatelů“*[53]

3.6 Situace v době pandemie covid-19

Jak každý dobře ví, a jak již bylo zmíněno výše, poslední dva roky se potýkáme s obrovským celosvětovým problémem způsobeným šířením viru COVID-19. Pandemie způsobená tímto onemocnění zasáhla určitým způsobem každého z nás. Restrikce a opatření spojená se snahou zabránit šíření této nákazy byly zaměřeny zejména na omezení sociálního kontaktu a interakce mezi lidmi. Tím způsobily, že téměř veškerá komunikace se přesunula do prostředí sociálních sítí. Stejně tak seznamování se, navazování kontaktů, ale i vyučování probíhalo, v době největších omezení, na internetu prostřednictvím sociálních sítí. Nejen že tím byl způsoben nárůst počtu uživatelů a hodin strávených on-line. Konkrétně v roce 2019, tedy než vypukla pandemie, byly k internetu připojeny 4,1 miliardy uživatelů což se, jak již bylo uvedeno, zvýšilo na 4,9 miliard připojených lidí v roce 2021.[54] Zvýšil se ale i počet obětí nejrůznějších útoků na sociálních sítích, jak také potvrzuje expert na tuto problematiku v rozhovoru, který je součástí praktické části této práce.

Nejvíce narostl počet obětí vyhrožování, kterými jsou zejména lékaři a představitelé vlády. Ve většině případů jsou důvodem přijatá opatření či přesvědčování lidí k očkování proti COVIDU-19. Jako příklad bych ráda uvedla

[53] Hoax. *Internetem bezpečně* [online]. [cit. 2022-02-13]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/hoax/#1492560436505-570636f0-92f1412b-edf227c5-c79da29b-5208

[54] RODRIGUEZ, Cecilia. Třetina lidstva nikdy nespatřila internet. Proč jsou tři miliardy lidí stále offline?. *Forbes* [online]. 27.12.2021 [cit. 2022-03-03]. Dostupné z: https://forbes.cz/tretina-svetove-populace-nikdy-nespatrila-internet-proc-jsou-skoro-tri-miliardy-lidi-stale-offline/

případ, kdy neznámý muž vyhrožoval bývalému premiérovi Andreji Babišovi usmrcením jeho i rodiny zastřelením, a to kvůli postupům při řešení zmíněné pandemie. Pachatel byl dopaden a jelikož se jedná o trestný čin hrozí mu trest odnětí svobody.[55] Policie ČR zveřejnila na svém Twitteru následující prohlášení: „*Policie ČR vnímá sílící útoky a projevy agresivity vůči autoritám z oboru zdravotnictví, ústavním činitelům i zdravotnickému personálu. Pachatele 4 z 5 mediálně známých útoků, ke kterým došlo v posledních dnech, jsme dopadli a vedeme s nimi řízení. Speciální týmy kriminalistů také stále monitorují kyber prostředí a v této souvislosti už stíháme desítky "internetových hrdinů", kterým za nebezpečné vyhrožování hrozí až 3 roky za mřížemi."*[56]

A, jak již bylo zmíněno v předchozí kapitole, v této nepříznivé době se též zvýšil počet falešných prohlášení, tzv. hoaxů, týkajících se zejména očkování proti COVIDU-19, šířících se po sociálních sítích.

Právní zakotvení forem všech výše zmíněných útoků bude předmětem následující kapitoly.

[55] Muž obviněný z vyhrožování Babišovi mu zaslal omluvu. Odpustil jsem mu, říká premiér. *Aktuálně.cz* [online]. Česká tisková kancelář, 15.4.2021 [cit. 2022-01-02]. Dostupné z: https://zpravy.aktualne.cz/domaci/muz-obvineny-z-vyhrozovani-babisovi-mu-zaslal-omluvu/r~f4da99409dda11ebb9860cc47ab5f122/

[56] Policie ČR. *Twitter* [online]. 3.12.2021 [cit. 2022-01-02]. Dostupné z: https://twitter.com/PolicieCZ/status/1466730134891909125

4 Právní zakotvení kriminality páchané na internetu

V této kapitole bude uvedeno, jak jsou v zákoně ustanoveny jednotlivé trestné činy realizované na sociálních sítích. Základním právním předpisem, ve kterém je zakotvena většina projevů daných útoků je trestní zákoník.

- Kyberšikana

Jako první útok byla popsána kyberšikana, která jako taková v zákoně sice upravena není, ale existují předpisy, které se jí zabývají. V trestním zákoníku jsou zakotveny například následující činy:

§ 144 Účast na sebevraždě

§ 145 Těžké ublížení na zdraví

§ 146 Ublížení na zdraví

§ 175 Vydírání

§ 180 Neoprávněné nakládání s osobními údaji

§ 181 Poškození cizích práv

§ 182 Porušení tajemství dopravovaných zpráv

§ 183 Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí

§ 184 Pomluva

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

§ 231 Opatření a přechovávání přístupného zařízení a hesla k počítačovému systému a jiných takových dat

§ 352 Násilí proti skupině obyvatelů a proti jednotlivci

§ 354 Nebezpečné pronásledování.[57]

- Kybergrooming

Kybergrooming máme opět zanesený v trestním zákoníku. Trest hrozí pachateli například za trestné činy uvedeny v tomto zákoně pod paragrafy:

§ 171 Omezování osobní svobody

§ 175 Vydírání

§ 185 Znásilnění

§ 187 Pohlavní zneužívání

§ 193b Navazování nedovolených kontaktů s dítětem

[57] Zákon č. 40/2009 Sb., *trestní zákoník v posledním znění*

§ 201 Ohrožování výchovy dítěte

§ 202 Svádění k pohlavnímu styku

§ 353 Nebezpečné vyhrožování.[58]

- Sexting

Sextingem může být zákon porušován například následujícími trestnými činy, které jsou zakotveny taktéž v trestním zákoníku:

§ 175 Vydírání

§ 186 Sexuální nátlak

§ 192 Výroba a jiné nakládání s dětskou pornografií

§ 193 Zneužití dítěte k výrobě pornografie

§ 193a Účast na pornografickém představení

§ 201 Ohrožování výchovy dítěte.[59]

- Phishing

Phishing může být trestán podle paragrafů trestního zákoníku:

§ 209 Podvod

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

§ 231 Opatření a přechovávání přístupného zařízení a hesla k počítačovému systému a jiných takových dat.[60]

- Hoaxy

I Hoaxy jsou od roku 2009 zakotveny v trestním zákoníku pod paragrafem:

§ 357 Šíření poplašné zprávy.[61]

Veškeré trestné činy výše zmíněné jsou trestány odnětím svobody pachatele. Míra trestu závisí na závažnosti provedeného činu a na tom, na kom byl trestný čin spáchán. Pří spáchání některého z výše uvedených činů například na dítěti, bude sazba automaticky vyšší.[62]

[58] Zákon č. 40/2009 Sb., *trestní zákoník v posledním znění*
[59] Tamtéž
[60] Tamtéž
[61] Tamtéž
[62] Tamtéž

5 Prevence v oblasti užívání sociálních sítí

Na začátku této kapitoly budou čtenáři seznámeni s příklady doporučení, jak by se zejména děti, ale i všichni uživatelé sociálních sítí, měli na sociálních sítích chovat a co by neměli dělat, a to podle knihy Thorstena Petrowskeho Bezpečí na internetu: pro všechny:

- *„Děti by na různých chatovacích fórech a sociálních sítích nikdy neměly prozrazovat kompletní údaje o své osobě, především adresu, telefonní číslo, nebo školu a třídu, kam chodí.*
- *Nikdy by neměly cizím lidem posílat své fotografie, ani ty nejnevinnější.*
- *Důležité je si uvědomovat, že na internetu se každý může snadno skrývat za falešnou identitou.*
- *Nikdy si nesjednávat schůzky přes internet.“*[63]

Cílem prevence je zejména předcházet nebo zmírňovat negativní jevy a jejich dopady. Můžeme ji rozdělit na primární, sekundární a terciární. Snahou primární prevence je předcházet nežádoucímu chování, v tomto případě na internetu. To znamená snaha o to, aby k rizikovému jednání vůbec nedošlo. Sekundární prevence má za úkol zareagovat na daný, již existující, nežádoucí jev v čas a zabránit jeho pokračování. Terciární prevence slouží k zajištění toho, aby se daný problém již neopakoval.[64]

Základní a tu nejdůležitější roli v prevenci v oblasti užívání sociálních sítí hraje rodina. Je důležité, aby rodiče mluvili se svými dětmi od útlého věku o rizikách, která hrozí na sociálních sítích, a jak se jim vyhnout. Sdělit jim, že ne všechno, co na internetu uvidí je pravda, a že ne každý je ten, za koho se vydává. Jak uvádí ve své knize Maria Vašutová a kol. podle Aleše Kavalíra, *„tak jako připravujeme své děti na to, aby zvládly nástrahy skutečného světa, musíme je naučit překonávat i problémy, s nimiž se mohou setkat ve světě virtuálním.“*[65]

---

[63] PETROWSKI, Thorsten. *Bezpečí na internetu: pro všechny*. Liberec: Dialog, 2014. Tajemství (Dialog). ISBN 978-80-7424-066-9. s. 70

[64] PAVLAS MARTANOVÁ, Veronika. O PRIMÁRNÍ PREVENCI RIZIKOVÉHO CHOVÁNÍ. *Národní ústav pro vzdělávání* [online]. květen 2014 [cit. 2022-03-01]. Dostupné z: https://www.nuv.cz/t/co-je-skolska-primarni-prevence-rizikoveho-chovani

[65] VAŠUTOVÁ, Maria. *Proměny šikany ve světě nových médií*. Ostrava: Filozofická fakulta Ostravské univerzity v Ostravě, 2010. ISBN 978-80-7368-858-5. s. 100.

Druhou, také velmi důležitou, úlohu v oblasti prevence hraje škola. Pokud dítě nemá oporu a důvěru ve svých rodičích je potřeba, aby škola sloužila jako podpora a místo, kde se dítě může svěřit s problémy, které prožívá nejen na internetu. V rámci školy je velice důležité, jak uvádí Maria Vašutová ve své knize Proměny šikany ve světě nových médií:

- *„Posilovat empatii u žáků.*
- *Zlepšovat atmosféru ve třídě.*
- *Vést k úctě vůči druhým.*
- *Dávat pozitivní zpětnou vazbu.*
- *Vytvářet dobré vztahy mezi učiteli a žáky.“*[66]

Existuje i mnoho projektů, které se zaměřují na prevenci, ale i řešení jednotlivých jevů vyskytujících se nejen na sociálních sítích. Mezi nejznámější patří:

- E-Bezpečí
- Linka bezpečí, Rodičovská linka
- Dětské krizové centrum
- Bílý kruh bezpečí[67]

Všechny tyto projekty se specializují na pomoc dětem a dospívajícím nebo studentům při prožívání nežádoucích jevů na internetu, které na ně mohou působit negativně. Výjimkou je Rodičovská linka, která slouží nejen pro rodiče, ale i pro jiné příbuzné či učitele potenciálních nebo existujících obětí a Bílý kruh bezpečí, který je určen pro všechny a jeho pracovníci jsou schopni pomoci při téměř jakémkoliv problému obětí trestných činů.[68]

[66] VAŠUTOVÁ, Maria. *Proměny šikany ve světě nových médií*. Ostrava: Filozofická fakulta Ostravské univerzity v Ostravě, 2010. ISBN 978-80-7368-858-5. s. 103.
[67] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3. s. 146-151
[68] Tamtéž. s. 146-152.

6 Budoucnost sociálních sítí

Jak budou sociální sítě vypadat do (ať už bližší nebo vzdálenější) budoucnosti, je jedna ze zásadních otázek, které se v dnešní době probírají. Existuje mnoho názorů a spekulací, jak by to mohlo se sociálními sítěmi být do budoucna, nikdo to však nedokáže říct s jistotou.

Velkou roli hrají obrovské společnosti a jednotliví vývojáři těchto technologií. V současné době je nejaktuálnějším projektem tzv. metaverse. Pojem metaverse, nebo také metaverzum, existuje již několik desítek let, ale technologie spadající pod tento pojem nejsou ještě úplně vyvinuty. V současnosti se tohoto záměru snaží dosáhnout mnoho společností, které se zapojují do zmíněného projektu, například i v daleké Číně. Nejblíže je tomu však Mark Zuckerberg, který také z toho důvodu v nedávné době přejmenoval společnost Facebook na Meta Platforms Inc., pod kterou spadá ale i Instagram, WhatsApp, Messenger a další.[69] Jedná se tedy o společnost obrovských rozměrů a nezměřitelného dosahu, která s jistotou ovlivní budoucí vývoj sociálních sítí. Co si ale pod pojmem metaverse představit? Přesná definice tohoto jevu zatím neexistuje. *„Zuckerberg jej popsal jako virtuální 3D prostředí, do kterého můžete vstoupit místo pouhého sledování ploché obrazovky. Jedná se o svět neomezených možností, vzájemně propojených komunit, míst pro virtuální setkání, pro práci i zábavu.“*[70] Skrz toto online prostředí, do kterého se člověk bude moci přenést, bude možno také například nakupovat, online cestovat, navštěvovat online koncerty, ale i využívat právě sociální sítě. Dá se říct, že člověk bude moci dělat úplně všechno jako před tím, jen s tím rozdílem, že to bude vykonávat z gauče u něj v obývacím pokoji.[71] Otázkou je, zda je to dobré, zda to nepřinese více negativních aspektů, než těch pozitivních a zda je to to, co opravdu každý chce. Na tuto otázku si ale musí už každý odpovědět sám.

[69] KOS, Adam. Meta: Vše, co byste měli vědět o přejmenovaném Facebooku. *Jablíčkář* [online]. 29.10.2021 [cit. 2022-02-20]. Dostupné z: https://jablickar.cz/meta/
[70] VRCHOTA, Matouš. Co je to metaverse? A proč v něm Facebook alias Meta vidí svou budoucnost?. *Inteligentní svět* [online]. 2.11.2021 [cit. 2022-02-20]. Dostupné z: https://inteligentnisvet.cz/clanky/co-je-to-metaverse-proc-je-to-budoucnost-firmy-facebook-meta
[71] Tamtéž

Expert na kybernetickou trestnou činnost na linii mravnosti se specializací na sociální sítě a dětskou pornografii Mgr. Marek Pačmag, MBA, LL.M. vidí budoucnost sociálních sítí následovně:

„Myslím si, že nárůst sociálních sítí a celkových aktivit na nich bude skutečně masivní. Respektive bych mohl říct, že to už nebude sdílení nějakých zážitků, ale to už bude live streamování celého jejich dne, potažmo celého jejich života. Tzn., že se to vyvine tak, že každý pojede ten svůj live stream a bude doufat, že bude natolik zajímavý, že se na něj budou dívat ostatní lidé. Prakticky to bude přenos celého dne těch lidí. Bojím se tady toho, že to v horizontu třeba dvou let skutečně nastane. Pokud to není částečně již dneska… Takže i v případě útoků na sociálních sítích bude skutečně nárůst, i přes to, že prevence je na mnohem lepší úrovni, než byla dříve.“

V každém případě můžeme říci, že co se týče sociálních sítí, čísla půjdou nahoru a pravděpodobně věková hranice uživatelů klesne směrem dolů. S tím samozřejmě přijdou i rizika. Mohou přijít nová rizika, se kterými se v dnešní době prozatím nesetkáváme nebo může být rapidní nárůst těch, které již známe. Proto je, společně s vývojem nových technologií a možností, potřeba zaměřit se na prevenci nežádoucích jevů na těchto platformách a snažit se jim co nejefektivněji předcházet.

II. PRAKTICKÁ ČÁST

7 Kvalitativní výzkum – řízený strukturovaný rozhovor

Pro účely praktické části této práce byl zvolen řízený strukturovaný rozhovor. Tento typ rozhovoru je jednou z metod kvalitativního výzkumu a vyznačuje se tím, že tazatel má předem přesně stanovené otázky, které při rozhovoru klade v daném pořadí. Otázky pro rozhovor s oběťmi jsou formulovány tak, aby zjistily jejich aktivitu na sociálních sítích – na kolika sociálních sítích mají účet, kolik času na nich tráví, jaké činnosti na nich vyvíjejí apod. Druhá část rozhovoru obsahuje otázky zaměřující se na daný útok, v obou zahrnutých případech se jedná o formu kyberšikany, konkrétně o „vydávání se za někoho jiného a krádež hesla“. Cílem těchto rozhovorů je zejména zjistit závadová jednání obětí a zaměřit se tak na možnosti prevence. Zároveň představit reálnost tohoto útoku, popsaného také v teoretické části práce, a jeho závažnost na skutečných příbězích. V případě rozhovoru s expertem na danou problematiku Mgr. Markem Pačmagem, MBA, LL.M., jsou otázky sestaveny tak, aby byly potvrzeny a případně doplněny fakta popsány v teoretické části této práce odborníkem se zkušenostmi z praxe, ze kterých budou následně taktéž vytvořeny závěry se zaměřením na možnost prevence rizik na sociálních sítích.

Pro zpestření a vyzkoušení popsané teorie v praxi je do následujících rozhovorů zahrnut i test na závislost na internetu, sestavený Lukasem Blinkou a Davidem Šmahelem z knihy Anny Ševčíkové Děti a dospívající online: vybraná rizika používání internetu, zmíněný v teoretické části této práce.

7.1 Rozhovor číslo 1 – oběť kyberšikany

Jako první jsem respondentce číslo jedna udělala orientační test na závislost na internetu, který dopadl následovně:

Pro první dvě otázky, tedy zda někdy zanedbává své potřeby kvůli internetu a zda si představuje, že je na internetu, i když na něm právě není, vybrala možnost **zřídka**. Následovala otázka zjišťující, zda se ji stává, že je na internetu výrazně déle, než původně zamýšlela, na kterou odpověděla **často**. To byli otázky vztahující se k první dimenzi význačnosti. Ke druhé dimenzi tolerance padly dvě otázky, tedy zda má pocit, že na internetu tráví stále více a více času a jestli se

někdy přistihne, že brouzdá po internetu, i když ji to už nebaví, na které odpověděla **často**. Dále byla položena otázka spadající do dimenze změn nálad, a to, zda se cítí veselejší a šťastnější, když se dostane konečně na internet, na kterou odpověděla **velmi často**. Na otázku z dimenze abstinenčních příznaků, zda se cítí neklidná, mrzutá nebo podrážděná, když nemůže být online odpověděla **často**. Pro otázku řadící se do dimenze relapsu, zda se někdy pokusila neúspěšně omezit čas, který je na internetu vybrala možnost **zřídka**. Na poslední dvě otázky náležící pod dimenzi konfliktu, tedy zda se někdy hádá se svými blízkými kvůli času, který tráví na internetu a zda její rodina, přátelé, práce, či zájmy strádají kvůli času, který tráví na internetu odpověděla, že **nikdy**.

Jak jsme se dozvěděli v teoretické části této práce, konkrétně v kapitole zabývající se závislostí na internetu, pro to, aby se daný jedinec mohl považovat za závislého na internetu je třeba mít v každé z dimenzí alespoň jednou odpověď často nebo velmi často. Z odpovědí výše tedy můžeme vyvodit, že respondentka číslo jedna nesplňuje podmínky pro orientační zařazení mezi závislé na internetu.

Následuje již samotný rozhovor zahrnující dvacet tři otázek.

1. *Byl/a jste seznámen/a se všemi podmínkami tohoto rozhovoru, zavazujete se k jejich plnění a můžeme tedy začít?*

Ano

2. *Kolik je Vám let?*

Je mi 15 let.

3. *Jaké je Vaše pohlaví?*

Jsem žena.

4. *Na kolika a jakých sociálních sítích máte založený účet?*

Asi na sedmi – na Instagramu, Snapchatu, Pinterestu, TikToku a na YouTube a pak ještě na WhatsAppu a Messengeru, ale tady máme třídní skupinu, takže to využívám jen pro tyhle účely. A messenger mám bez Facebooku.

5. *V kolika letech jste si založil/a svůj první účet na sociální síti a na jaké?*

V deseti letech na Instagramu a Musical.ly.

6. *Kolik času denně trávíte na sociálních sítích?*

Tak tři až čtyři hodiny.

7. *Jaké činnosti na těchto sítích nejčastěji děláte?*

Na TikToku projíždím videa, na YouTube poslouchám písničky a na Instagramu si prohlížím fotky.

8. *Upřednostňujete on-line či off-line komunikaci?*

Určitě off-line komunikaci z očí do očí.

9. *Na jaké sociální síti se útok odehrál?*

Na tehdejším Musical.ly, předchůdce TikToku.

10. *Kolik přátel jste měl/a na této sociální síti?*

Já jsem na této sociální síti sledovala asi deset lidí a mě sledovalo zhruba dvacet lidí.

11. *Kolik z nich jste znala osobně?*

Osobně jsem znala většinu z nich, až na výjimky, které jsem věděla, že se, stejně jako já, zajímají o koně a přidávají na této sociální síti věci týkající se právě koní.

12. *Kolik Vám bylo, když se útok odehrál?*

Bylo mi deset let.

13. *Jaký byl Váš vztah k útočníkovi?*

Byla to moje nejlepší kamarádka a zároveň spolužačka.

14. *Jak útok probíhal?*

Moje tehdejší nejlepší kamarádka znala heslo k mému účtu. Tenkrát jsme se o tom bavily a navzájem jsme si ho řekly, nikdy by mě nenapadlo, že by toho zneužila, že by něco takového udělala. No pak jsme se ale pohádaly a ona mi vlezla do toho účtu, smazala mi moje videa a nahrála tam svoje, kde ale nebyla vidět. Byla tam vždycky třeba jen ruka nebo zeď a u toho byl popisek typu „jsem píča“. Taky mi do bia napsala, že si o sobě myslím, že jsem „píča, kráva, mrdka,…“ a podobně a změnila i fotku, kde byla zase jenom ruka. Ale heslo k tomu účtu nezměnila, takže já, když jsem se přihlásila, tak jsem jen koukala, co se to děje, hrozně jsem se lekla.

15. *Jak dlouho útok trval?*

Trvalo to asi pět dní, než jsem to zjistila a začala to řešit.

16. *Jak jste to řešil/a?*

Hned jak jsem to zjistila, tak jsem to řekla mamce. Když jsme ji potom kontaktovali, jestli to byla ona, tak byla hrozně nervózní, tvrdila, že to nebyla ona, že to byli „hateři“, že by to v životě neudělala. Hrozně se bála mamky, vyhýbala se ji, když

ji viděla, tak přecházela chodník. Pak jsem si tu sociální síť smazala, vlastně jsem si smazala všechny sociální sítě, protože jsem měla strach. S tou kamarádkou jsem se přestala bavit a od té doby se už ani nezdravíme. A víc už jsem to neřešila.

17. *Jak jste zjistil/a, kdo byl pachatelem?*

Nejdřív jsem nevěděla, kdo to byl, když jsme to pak ale s mamkou prozkoumávali víc, došlo nám, že to byla ona. Ona si vlastně úplně hloupě dala „like“ z toho mého účtu ke všem svým videím, což já vím, že jsem já nebyla. Takže tak jsem na to přišla.

18. *Jak na to reagovali rodiče?*

Mamce jsem to řekla hned, jak jsem na to přišla, ta se vyděsila, nechápala, co se to stalo a pak když nás vezla z gymnastiky, kam jsme spolu chodily, tak se ji na to zeptala, jestli to byla ona. Ona byla hrozně ve stresu, roztěkaná. Když se jí mamka zeptala, proč to udělala, tak neodpověděla.

19. *Jak se k tomu postavila škola?*

Se školou jsme to vůbec neřešili.

20. *Jaký to na Vás mělo dopad?*

V tu dobu jsem z toho byla hodně špatná. Protože i ve škole o mě začala šířit pomluvy, aby nás ve třídě rozdělila a přetáhla si lidi na svoji stranu. Ironie je, že teď chodím do třídy s jednou holčinou, právě z té druhé party, se kterou jsme na sebe koukaly skrz prsty kvůli ní, tak teď jsme nejlepší kamarádky. A asi měsíc jsem z toho byla fakt špatná, ale i potom, když jsem na to pomyslela, tak jsem furt byla taková, že jsem si to vybavila znova a byla jsem z toho znovu špatná.

21. *Vnímáte následky ještě dnes? Jaké?*

Vůbec ne, teď už se tomu směju.

22. *Jste i po útoku aktivní na dané sociální síti?*

Dneska už jo, ale jak už jsem říkala, hned po tom, co se to stalo, jsem si tu sociální síť smazala, vlastně všechny sociální sítě, které jsem v té době měla a asi půl roku jsem si na žádné účet nezaložila, protože jsem se bála. Na novém účtu, který mám tedy už na TikToku, tak mám soukromý účet, vlastně všechny účty už mám soukromé a na žádné ji nemám v přátelích. Od té doby ale nepřidávám žádná videa na TikTok a na Instagramu mám jen pár fotek, které vidí jen několik lidí, kterým to povolím, jinak fakt vůbec nikam nic nepřidávám. Já jsem si asi úplně dřív neuvědomovala ten dopad, toho, co se děje na sociálních sítích, nebo co se může

stát. Teď už si, možná i částečně díky tomu, uvědomuju ty rizika a nikomu bych nesdělila svoje údaje ani bych neměla veřejný účet a nepotvrzuji žádosti o sledování nikomu koho neznám nebo se mnou nesdílí mé zájmy, což jsou koně.

23. *Měli jste v rámci školy organizované nějaké aktivity, které by Vás upozornily na rizika na sociálních sítích?*

Na základní škole jsme měli v rámci občanské výchovy přednášku od odborníka na toto téma, a i učitelé nám o tom říkali. Teď na střední jsme v rámci hodiny informatiky koukali na interaktivní video, kde nám o tom povídali a sami jsme se i zapojovali. Nic nového jsem se ale nedozvěděla, ve většině případů to byly věci, které už jsem znala.

7.2 Rozhovor číslo 2 – oběť kyberšikany

Stejně jako u předchozí respondentky i v tomto případě byl na začátku rozhovoru vykonán úplně stejný test na závislost na internetu obsahující tytéž otázky. Proto otázky nebudou již zmiňovány, budou vypsány pouze odpovědi na ně. Na první tři otázky v dimenzi význačnosti respondent odpověděl **často**, **zřídka** a **velmi často**. Na čtvrtou a pátou otázku spadající do dimenze tolerance odpověděl **často** a **velmi často**. Pro šestou otázku v dimenzi změn nálad vybral možnost **nikdy** a na sedmou otázku náležící do dimenze abstinenčních příznaků odpověděl **zřídka**. Na následující otázku z dimenze relapsu odpověděl **často** a na poslední dvě otázky z dimenze konfliktu odpověděl **nikdy** a **často**. Zde opět můžeme konstatovat, že respondenta nelze považovat za závislého na internetu, neboť nesplňuje již zmíněné podmínky.

Následuje samotný rozhovor opět obsahující stejných dvacet tři otázek jako u předchozí oběti.

1. *Byl/a jste seznámen/a se všemi podmínkami tohoto rozhovoru, zavazujete se k jejich plnění a můžeme tedy začít?*

Ano

2. *Kolik je Vám let?*

Je mi 23 let.

3. *Jaké je Vaše pohlaví?*

Jsem muž.

4. *Na kolika a jakých sociálních sítích máte založený účet?*

Asi kolem devíti. Tinder, Badoo, Bumble, Facebook, Instagram, BeReal, YouTube, WhatsApp, a pak ještě Twitter, ten ale nepoužívám.

5. *V kolika letech jste si založil/a svůj první účet na sociální síti a na jaké?*

Na Facebooku a bylo mi dvanáct.

6. *Kolik času denně trávíte na sociálních sítích?*

Dohromady tak dvě hodiny, spíš trávím čas koukáním na Netflix a hraním PlayStationu.

7. *Jaké činnosti na těchto sítích nejčastěji děláte?*

Sleduju „storýčka“ jiných lidí, píšu si s lidmi, čtu si zajímavý články, hodně sleduju profily na téma osobnostního rozvoje a finanční gramotnosti a zajímám se o celosvětové novinky.

8. *Upřednostňujete on-line či off-line komunikaci?*

Rozhodně off-line.

9. *Na jaké sociální síti se útok odehrál?*

Na Facebooku.

10. *Kolik přátel jste měl/a na této sociální síti?*

Tak sto padesát.

11. *Kolik z nich jste znala osobně?*

Zhruba třetinu z nich. V té době jsme se s kamarády předháněli, kdo bude mít víc přátel, takže jsem si přidával i lidi, které jsem neznal.

12. *Kolik Vám bylo, když se útok odehrál?*

Bylo mi dvanáct.

13. *Jaký byl Váš vztah k útočníkovi?*

Chodil jsem s ní. Byla to moje holka.

14. *Jak útok probíhal?*

Já jsem do vztahu s ní vstupovat nechtěl, ale v té době jsem nevěděl, jak zareagovat a vstoupil jsem s ní do vztahu a ona to brala velmi vážně. Já jsem to chtěl po nějaké době ukončit, ale ona mi řekla, že spáchá sebevraždu, když se rozejdeme. Takže jsem nevěděl, co dělat a potom jsem jí začal ignorovat a ona pak přišla, že je mezi námi konec. Tak jsem byl v pohodě s tím a odsouhlasil to, jenže ona mě jen zkoušela, chtěla vidět moji reakci a naštvala se. V tu chvíli se na mě strhla lavina urážek a ponižování na Facebooku od ní a od jejích třech kamarádek. Například mi sdílely na zeď fotku mrtvého holuba a psaly pod to, jak

bych si na tom pochutnal a tak. Psaly mi hnusné zprávy a komentáře pod fotky a příspěvky, třeba že jsem špína a přirovnávaly mě k odporným věcem. A vygradovalo to tím, že mi vlezla na Facebook, jelikož znala moje heslo k Facebooku, protože jsme si ho řekl, a napsala klukům z deváté třídy ošklivé zprávy pod fotky a cíleně vyvolala konflikt. Ti kluci mě potom chtěli ve škole zmlátit. Já jsem se kvůli tomu ve škole rozbrečel.

15. Jak dlouho útok trval?

Zhruba dva týdny, než jsem zjistil, že ti kluci mě chtějí zmlátit kvůli tomu, že jim někdo z mého účtu psal hnusné zprávy a komentáře.

16. Jak jste to řešil/a?

Řekl jsem to učitelce ve škole, co se stalo a ti kluci se mi potom omluvili a ty holky to potom přestaly dělat, hlavně proto, že jsem si změnil heslo k mému účtu.

17. Jak jste zjistil/a, kdo byl pachatelem? Jak na to reagoval/a?

Mně to bylo jasný po tom, co mi posílaly a nadávaly mi. Oni se tím bavily, byla to pro ně sranda.

18. Jak na to reagovali rodiče?

Rodiče to vůbec nevěděli.

19. Jak se k tomu postavila škola?

Jediný co, tak se o tom bavili všichni učitelé a každý třídní učitel potom upozorňoval na problematiku kyberšikany před začátkem jejich hodiny.

20. Jaký to na Vás mělo dopad?

Hodně jsem se poučil, ale zároveň jsem pak už nechtěl mít s holkami nic společného a už vůbec ne s někým chodit. Až do deváté třídy.

21. Vnímáte následky ještě dnes? Jaké?

Ne, už je to dávno a asi kdybych se s tou holkou teď potkal, tak si s ní normálně povídám. Byly jsme děti…

22. Jste i po útoku aktivní na dané sociální síti?

Ano, ale určitě bych už nikomu nesdělil svoje přístupové údaje.

23. Měli jste v rámci školy organizované nějaké aktivity, které by Vás upozornily na rizika na sociálních sítích?

Na nic si nevzpomínám. Já osobně jsem o tom nic nevěděl. Já ani nevěděl, že se v tom mém případě jedná o kyberšikanu. K nám často chodili odborníci povídat na téma finanční gramotnosti nebo sexuální výchovy, ale nic takového si nevybavuju.

7.3 Rozhovor číslo 3 – expert na danou problematiku

Tento rozhovor byl vykonán s Mgr. Markem Pačmagem, MBA, LL.M. a obsahuje osmnáct otázek zaměřených zejména na zjištění informací o nejčastěji páchaných útocích na sociálních sítích v České republice, dále o obětech, o agresorech a také o situaci na sociálních sítích v době pandemie COVID-19. Na závěr jsou kladeny otázky zaměřené na právní zakotvení útoků na sociálních sítích a na doporučení samotného experta uživatelům sociálních sítí, jak se nejlépe útokům vyhnout.

1. *Byl/a jste seznámen/a se všemi podmínkami tohoto rozhovoru a zavazujete se k jejich plnění?*

Ano

2. *Mohl/a byste se tedy prosím představit?*

Působím na Policejním prezidiu na úřadu služby kriminální policie a vyšetřování na linii mravnosti se specializací na sociální sítě a dětskou pornografii. Vystudoval jsem Policejní akademii České republiky v Praze v magisterském stupni studia a v současné době jsem externím doktorandem na Českém vysokém učení technickém.

3. *Jak dlouho se touto problematikou zabýváte?*

Touto problematikou se zabývám již od roku 2014, kdy v této době bylo užívání sociálních sítí už relativně rozšířeno, ale páchání trestné činnosti na nich nebylo tak časté jako v dnešní době.

4. *Které útoky řešíte nejčastěji, a které jsou méně časté?*

Velmi aktuální a poměrně časté jsou případy odcizení uživatelských účtů na různých sociálních sítích, převážně však na Facebook (dnes META). K samotnému odcizení účtu dochází tak, že uživatelé jsou přesměrováni na fiktivní stránku pomocí odkazů s nějakým pro ně zajímavým obsahem, kde jsou následně vyzváni k opětovnému přihlášení k účtu, čímž sdělí přístupová hesla útočníkovi, který tím dostane přístup k účtu a může s ním podle vlastního uvážení dále nakládat. Osobně se domnívám, že to lze označit za druh phishingového útoku, protože se jedná o uvádění druhých v omyl a vylákání přihlašovacích údajů. Je to v podstatě to samé, jako rozesílání odkazů na fiktivní stránky bankovních institutů, které byly moderní třeba 3-4 roky nazpět.

Co se týče kyberšikany, nejfrekventovanější útoky jsou v současné době mezi žáky navzájem, kdy se například ve třídě natočí nějaké dehonestující video a inkriminovaná osoba je následně tímto způsobem šikanována v prostředí internetu. Nicméně objevují se i případy, kdy je kyberšikanován učitel, tzn. že se skrytě při výuce pořídí nějaké video, které zachycuje předmětného učitele v nějaké nekomfortní nebo směšné pozici a pak následně je toto video umisťováno na sociální sítě a jsou pod ním přidávány komentáře jak ze strany žáků třídy, kde bylo video pořízeno, tak i ze strany dalších žáku školy, potažmo i žáků dalších škol. Dosah sociálních sítí je v dnešní době skutečně neomezený. Je těžké proti tomuto jevu bojovat, protože je to zpravidla umisťováno na zahraniční sociální sítě, ne české, tam je tedy jediná možnost, a to nahlásit závadový obsah a je jenom na provozovateli té konkrétní sociální sítě, zda tomuto nahlášení vyhoví a obsah smaže nebo ne.

Co se týče sextingu, je to v současné době také běžnou záležitostí a troufám si tvrdit, že málokdo si uvědomuje rizika sextingu. Je potřeba zmínit, že konsenzuální sexting mezi dospělými osobami je legitimní, ale pokud je do sextingu zapojeno dítě ne mladší patnácti let, jak je někdy mylně prezentováno, ale mladší osmnácti let, tak samozřejmě je pak možno takové jednání kvalifikovat například jako trestný čin zneužití dítěte k výrobě dětské pornografie, popřípadě šíření pornografie a další trestné činy.

Co se týče kybergroomingu, jedná se o méně často se vyskytující jev než sexting. Kybergrooming je potřeba rozdělit do dvou forem. Grooming, kde dochází k nějaké dohodě, ale k setkání fakticky nedojde a pak grooming, kde dojde k dohodě i k následnému setkání, které je samozřejmě mnohem více rizikové. Kdybych měl tedy porovnat sexting a kybergrooming, tak sexting je častější, grooming je ale na druhou stranu, pokud dojde k setkání s útočníkem, závažnější.

5. *Jsou oběti ochotny bez problému probíhající útok nahlásit nebo si to spíše nechávají pro sebe?*

Záleží, čeho se to týká. Je potřeba zacílit na útoky do jednotlivých oblastí.

Co se týče podvodů, tzn. že pokud vás někdo přes sociální sítě podvede, vy pošlete předem finanční prostředky a přijdete o ně, tak to je oznamováno celkem často. Ti lidé nemají ostych říct, že se jim to stalo a přijít na policii podat oznámení. Co se týče tedy této trestné činnosti majetkové, tak tam není problém.

Co se týče třeba odcizení účtu, tam už to tak dobré není, protože v dnešní době si během chvilky založíte jiný účet a nechcete trávit čas na policejní stanici nahlašováním, že vám někdo odcizil účet, když ve vteřině můžete mít účet nový a vložíte do něj zcela stejné údaje, jaké byly v tom předchozím. Jediné, co je zde problém je, když vám někdo odcizí účet a začne psát uživatelům, které máte v přátelích. To je jeden z důvodů, proč lidé nakonec přijdou, protože se dostávají do linie poškozených i jejich přátelé.

Nejméně často je pak oznamován sexting, protože jednotlivé osoby, které by tou činností měly být poškozeny, se snaží to nechat dlouho na poli latence, aby se o tom nikdo nedozvěděl, zejména rodiče, spolužáci či kamarádi. Ale pokud zde dochází k nějakým výhružkám, tzn. že osobě začne někdo hrozit například „pošli další fotky nebo zveřejním ty co už mám“, což je takový ten nejznámější příběh, tak tam se ti poškození rozhodnou, že je potřeba to řešit a zmíní se ať už rodičům nebo ve škole nebo nejlepší kamarádce a pak už k tomu oznámení tedy dochází. Ale samozřejmě z prvopočátku je tam ta překážka toho, že ten poškozený nechce, aby se to dozvěděl někdo další.

6. *Která věková skupina je podle Vás nejohroženější a proč?*

Já se domnívám, že nejohroženější skupina je od osmi zhruba do patnácti let. Chtěl bych říct, že je to pouze můj odhad, nemám ho podložený žádným výzkumem. Nicméně je možné také uvést, že nejohroženější skupina jsou všichni, kdo mají sociální síť, tzn. že nelze určit tu spodní hranici, protože někdo má sociální síť, nebo přístup na sociální síť, už od šesti let věku. Takže já nemůžu teď říct, že je to přesně od osmi do patnácti let, neboť ta spodní hranice nelze určit. Každý má ten kupříkladu Facebook od jiného věku, byť konkrétně sociální síť je možné využívat až od třináctého roku věku. Samozřejmě je to individuální, každý je vyspělý jinak, přemýšlí u toho jinak, chce používat sociální sítě na jiné činnosti, takže nelze úplně říct je to od tehdy do tehdy, jak jsem řekl na začátku, ale spíš je to individuální.

7. *Kdo má největší sklony k tomu stát se obětí?*

V tomto směru je důležitým aspektem skutečnost, proč ty sociální sítě chce jedinec používat. Jestli je chce používat proto, že tam mají založenou například studijní skupinu a používá je jen v rámci tady té skupiny a přeposílají si tam studijní materiály, tak ten útok mu nehrozí tolik. Když to bude mít v rámci nahrazení

seznamky nebo bude chtít hodně chytat „followers“ nebo „lajky“ tam je samozřejmě možnost toho útoku mnohem vyšší, protože ti útočníci můžou zacílit na to, že se stará a jsou pro něj důležité tady ty atributy. Jednoznačně na to má ale vliv i rodina a sociální prostředí.

8. Jakou roli při řešení kyberšikany hraje škola?

Já si myslím, že v současné době všechny školy, které by se dozvěděly o kyberšikaně, tak opatření učiní. Je třeba říct, že se to neděje na půdě školy, neděje se to v době vyučování, je to někde v kyberprostoru a myslím si, že některé školy tímto argumentují, že se to děje v době osobního volna studentů a škola tady do těch věcí nijak nezasahuje. Ale pokud se o tom dozví, tak samozřejmě učiní opatření v podobě oznámení na policii.

9. Jaké dopady může mít na oběť sexting?

Opět je to velmi individuální. Pro někoho může být sexting zničující, co se týče budoucího zaměstnání, studia nebo osobního života. Pro někoho, kdo třeba nemá až takové ambice do budoucna, bavím se například o studentkách středních škol, které třeba skutečně nemají ty tendence nějaké extrémní kariéry, tak pro tu ten sexting třeba až tak zničující nebude, jako třeba pro dívku nebo chlapce, kteří mají ambice a chtějí něco dokázat a stane se jim to. Samozřejmě je notoricky známé, že všechno, co se objeví v prostředí internetu a opustí dosah oprávněného uživatele, tzn. že to někam přepošle, ať už cizímu člověku nebo partnerovi, tak bohužel to bude žít už na věky svůj život a nikdy nevíte, kdy se to objeví. Skutečně záleží, co to je za osobu, je třeba řešit to individuálně, ale ve finále lze konstatovat, že následky, co se týče sextingu a groomingu, pokud dojde k setkání a nedej bože k sexuálnímu zneužití, jsou nedozírné a oběti si je prakticky nesou celý život.

10. Mají tyto útoky dopad i na okolí oběti?

Nejbližší okolí oběti je určitě tímto zasaženo. Vezměte si například, když se to stane dívce, které je třináct let, tak samozřejmě pokud jde potom podávat vysvětlení na policii, tak nejbližší rodina to prožívá s ní. Zpravidla jdou rodiče s dívkou na tu policii jako psychická podpora. Pokud jsou pak třeba ve škole nějaké problémy, tak rodiče zase působí u oběti jako ten „polštář proti tomu nárazu“, ale skutečně to nejbližší okolí, zejména zákonní zástupci, blízká rodina, to prožívají stejně (někdy i mnohem více), než ta oběť.

11. V jaké míře bývají odhaleni pachatelé vzhledem k anonymitě online prostředí?

Neřekl bych úplně, že to je většina. Zejména s ohledem na to, že tyto útoky probíhají přes sociální sítě, jak bylo řečeno na začátku, zejména zahraniční, tak zde potom policejní orgán musí čekat poměrně dlouhou dobu, než informace k účtům pachatelů obdrží a samozřejmě čím dál se nacházíme od spáchaného skutku, tím klesá možnost chytit a usvědčit pachatele.

12. Kdo bývá nejčastěji pachatelem?

Opět je to individuální, protože někteří pachatelé mají zcela čistý trestní rejstřík, někteří pachatelé mají v rejstříku nějaký záznam, ale vůbec se netýká třeba mravnostní trestní činnosti, tzn. že byli odsouzení například za krádež, zanedbání povinné výživy a podobné trestné činy. Nachází se tam samozřejmě nějaká část pachatelů, kteří již v minulosti byli odsouzeni za sexuálně motivovanou trestnou činnost, a ti nám recidivují.

13. Jaká bývá motivace agresorů k uskutečnění útoku?

Jedna část pachatelů jsou ti, kteří ve svém dětství prožili nějaké trauma nebo nějakou negativní událost. Dále mě napadá motivace spočívající v tom, že to pachatel dělá pro vlastní uspokojení. Domnívám se, že takováto motivace převažuje, pokud se budeme bavit o sextingu nebo o nějakém sexuálním nátlaku samozřejmě i pokud se budeme bavit o groomingu, protože tam je také to setkání iniciováno za účelem následného sexuálního aktu, ale i samozřejmě dalších forem jednání. Takže si myslím, že velká část to dělá pro aktuální uspokojení.

14. Zvýšil se počet útoků na sociálních sítích v době pandemie covid-19?

V průběhu pandemie COVID 19, tzn. za poslední zhruba dva roky, tam pociťuji značný nárůst této kriminality. Tento nárůst je skutečně masivní, často o tom hovoří i veřejnoprávní a soukromoprávní média. Lidé nechodí tolik ven, tráví více času doma, a to je taková všeobecně známá notorieta, že za covidu této problematiky, jak již bylo uvedeno, masivně přibylo. S tím paralelně souvisí i užívání sociálních sítí ze strany mladších generací. V dnešní době, když se projdete po městě, tak takřka každý mladý drží v ruce mobilní telefon, pokud půjdete někam do kavárny, do knihovny, tak tam je to to samé, tzn. ta mladá generace je skutečně upnuta na informační a komunikační technologie zejména mobilní telefony, v dnešní době již nízkorozpočtové nástroje pro komunikaci.

15. *Jaká jsou podle vás pozitiva a negativa užívání sociálních sítí?*

Pokud se sociální sítě používají s rozmyslem a uživatelé u toho přemýšlejí, tak si myslím, že to je dobrá platforma pro komunikaci, rychlou komunikaci, komunikaci, která je zdarma. Na druhou stranu si myslím, že sociální sítě v současné době již neplní úplně tu funkci, proč byly vytvořeny. Byly vytvořeny pro komunikaci lidí s lidmi, kteří spolu nemohou být. V současné době se domnívám, že to je již jen prezentace rádoby hezkých chvil v životech jednotlivých uživatelů. V dnešní době sociální sítě slouží jako médium, které dokáže i některým vydělat nějaké finanční prostředky. Zde odkážu na všeobecně známé youtubery, kdy v dnešní době už se volá po tom, aby byly studijní programy na středních školách youtubering. Přijde mi to zajímavé. Samozřejmě lidé, kteří mají hodně „followers" asi skutečně mohou vydělat nějaké finanční prostředky a v současné době se mladší generaci líbí ta vize, že prakticky bez práce mohou přijít k finančním prostředkům. Je to pouze můj názor, ale já to takhle vnímám.

16. *Je podle Vás právní úprava týkající se útoků realizovaných na sociálních sítích dostačující?*

Co se týče trestního práva procesního, tak zde je skutečně potřeba reagovat na to, že velká část sociálních sítí je zahraniční a skutečně na informace k účtům pachatelů je mnohdy vyčkáváno velmi dlouho a po té době již nelze, nebo lze jen velmi těžko ustanovit konkrétního pachatele. Takže je potřeba, co se týče procesu tady to zakotvit. Samozřejmě se nejedná pouze o ČR, ale je potřeba to upravit na poli mezinárodním a pak následně v České republice. Co se týče trestního práva hmotného, tak ta právní úprava byla v posledních letech měněna. Byl zde nově přidán § 193b, tzn. nedovolené navazování kontaktu s dítětem, které vlastně je kybergroomingem. Co se týče sextingu ten tam je též zahrnut, pokud se jedná tedy o osoby, jak jsem již řekl mladší osmnácti let. Tady skutečně je potřeba si říct, že to je osmnácti let. Spousta občanů ČR si myslí, že dětská pornografie to je pouze u osob mladších patnácti let, což je prostě mylné, protože ve smyslu § 126 TZ je dítětem osoba mladší osmnácti let.

17. *Myslíte si, že je prevence v ČR zaměřená na rizika na sociálních sítích dostačující?*

Můžu říct, že co se týče prevence, tak ta je na mnohem vyšší úrovni, než bývala dříve. Skutečně těm rizikovým věkovým skupinám v rámci například přednášek na

základních školách nebo středních školách je prezentováno na příkladech z praxe, kam až může vyvrcholit takový útok v podobě sextingu nebo groomingu. Tím ale neříkám, že je plně dostačující, protože samozřejmě se dají vymýšlet nové projekty, ale myslím si, že všechny zainteresované subjekty se snaží a cítí tu potřebu lidem vysvětlovat, jaké jsou problematické aspekty na sociálních sítích a aby skutečně si dávali pozor, než něco například někam pošlou, tím myslím například intimní fotografie.

Myslím si, že zde musíme hodně zapracovat na rodičích jako jedné skupině, protože ty rodiče v rámci jejich rodičovské odpovědnosti by měli vědět, co jejich dítě dělá na sociálních sítích, jakou aktivitu tam vyvíjí a měli by samozřejmě umět zaprvé ty sociální sítě ovládat a měli by samozřejmě být schopni i nastavit případně tu sociální síť tak, aby byly ochráněny osobní údaje jednotlivých uživatelů. Takže myslím si, že zde bude velmi dobré, pokud se zacílíme jak na ty jednotlivé uživatele, ale také na rodiče, pokud tam ještě stále vyplývá rodičovská odpovědnost vůči jejich dítěti. A samozřejmě bych si uměl i představit, že do budoucna by mohl být na základních a středních školách vyvinut předmět, který by řešil právě tyto útoky a skutečně připravil děti na to, že se jim to může stát, tzn., že bych to dal buď jako nový předmět, nebo bych to subsumoval v rámci občanské nauky nebo něčeho podobného.

18. *Co byste Vy osobně doporučil/a uživatelům sociálních sítí, aby se takovýmto útokům vyhnuli?*

Aby začali na sociálních sítích přemýšlet, aby pochybovali o činnostech dalších uživatelů, které by se mohli vyvinout v útok, jejichž uživatelské účty vypadají zcela věrohodně.

7.4 Shrnutí výsledků kvalitativního výzkumu

Tato kapitola slouží zejména k tomu, aby byly shrnuty fakta zjištěny vykonanými rozhovory. Aby byla na jejich základě potvrzena či vyvrácena některá tvrzení z teoretické části této práce a aby byla zároveň vytyčena případná závadová jednání obětí, která vedla k jejich viktimizaci, z čehož mohou být následně vyvozeny závěry se zaměřením na prevenci.

Z výsledků testu na závislost na internetu, který byl vykonán na začátku obou rozhovorů, lze u obou obětí vyvodit, že na něm nebyli závislí ani v době útoku,

neboť obě oběti uvedli, že mají pocit, že tráví na internetu více a více času, a i přes to dnes nesplňují podmínky pro zařazení mezi závislé na internetu. To nám tedy tvrzení, že závislí na internetu jsou náchylnější k tomu stát se oběti nepotvrdilo, avšak ani nevyvrátilo, neboť se pro posouzení takového jevu jedná a malý vzorek respondentů.

První rozhovor byl vykonán se ženou, druhý s mužem. Z toho můžeme usoudit, že problematika rizik na sociálních sítích se týká obou pohlaví a nemůžeme je vztahovat jen k jednomu. U obou respondentů můžeme také vidět v současné době značnou aktivitu na mnoha sociálních sítích, včetně té, na které se útok odehrál. To naznačuje, že útok z minulosti je nijakým výrazným způsobem neodradil od jejich užívání.

Co se týče začátků respondentů na sociálních sítích můžeme vidět, že opravdu s postupem času se snižuje věková hranice zakládání si účtů na sociálních sítích. Respondent číslo dvě si založil svůj první účet v roce 2011, kdy sociální sítě, dá se říct, teprve začínaly a bylo mu v té době dvanáct let. Respondentka číslo jedna si založila svůj první účet v roce 2017 a bylo jí teprve deset let. Do budoucna lze tedy očekávat ještě větší snížení této věkové hranice.

Z pohledu činností, které respondenti vykonávají na sociálních sítích lze pozorovat, že je to rozdílné. Dle mého názoru zejména kvůli věkovému rozdílu. Mladší respondentka číslo jedna spíše ztrácí čas na sociálních sítích ničemu neprospívajícími činnostmi, kdežto starší respondent číslo dvě, mimo tyto stejné činnosti, se snaží vzdělávat a posouvat své znalosti a vědomosti a zajímá se o světové dění, což považuji za užitečné.

Co se týče samotných útoku a závadového jednání obětí lze shrnout následující:
U obou obětí se jednalo o tentýž útok, tudíž lze předpokládat, že u obou se jednalo o podobné chyby, kterých se dopustily. Tím největším pochybením bylo sdělení svých přístupových údajů, jím zdánlivě blízkým osobám. Samotná tato problematika je velice ošemetná a děti ve věku obětí v době, kdy se útoky odehrály jsou velice důvěřivé a ve většině případů nepředpokládají zneužití a zradu od blízkých osob.

U první respondentky je též velice nebezpečné jednání, které uvedla, a to to, že si do svých přátel přidávala a sledování potvrzovala i osobám, které neznala, a které s ní sdílely její zálibu v koních. Toho by mohl snadno zneužít kdejaký predátor. To se v jejím případě nestalo, ale v jiných případech by to mohla být příčina útoku. U druhé oběti je také velice zarážející, že znala pouze třetinu svých přátel na dané sociální síti.

První respondentka nám v rozhovoru stvrdila to, že rodina hraje velmi důležitou roli v oblasti prevence. Na druhou stranu druhý respondent nám potvrdil tvrzení z teoretické části, že je třeba dbát na roli školy při řešení útoků na sociálních sítích. Oběť neměla plnou oporu v rodičích, proto se jim s daným problémem nesvěřila, ale řekla to právě pedagogickým pracovníkům ve škole, kteří danou situaci zvládli vyřešit. Dle mého názoru by však bylo také vhodné uvědomit policii, aby agresorky vyvodily adekvátní následky svého ubohého jednání.

U první oběti se také potvrdilo tvrzení, že kyberšikana je bohužel často provázena klasickou šikanou a v případě druhé oběti, pokud by nedošlo k zásahu ze strany školy, lze předpokládat, že by ke klasické šikaně také došlo.

Co se týče dopadů na oběti, v obou případech to mělo samozřejmě na nějakou dobu negativní dopad, nejedná se však o dopad dlouhodobého rázu, což je samozřejmě pozitivní fakt.

Oba respondenti potvrdili, že se dostatečně poučili ze svých chyb a znovu by je už neopakovali. Také jsou díky těmto útokům obezřetnější a opatrnější.

Co se týče rozhovoru s expertem na danou problematiku, zjištěno bylo zejména to, že útoky směřované proti obětem zahrnutým v předchozích dvou rozhovorech jsou velice aktuální a časté. Ve většině případů se však do účtů dostanou agresoři pomocí podvodů. Odborník také uvedl, že časté jsou i jiné formy kyberšikany, směřující například i proti kantorům. Sexting je podle něho také velmi častým jevem, kdy nejzávažnější je ten, do kterého jsou zapojeny děti do osmnácti let.

Expert také potvrdil, že podle něj jsou nejohroženější věkovou skupinou děti od osmi do patnácti let, kam spadaly i oběti z mého rozhovoru v době útoku.

Samozřejmě je to individuální a lze podle něho říci, že ohroženou skupinou jsou všichni ti, kteří mají sociální sítě.

Jak již bylo zmíněno, respondenti rozhovorů v této práci nemají vážnější dlouhodobé následky. Co se ale týče sextingu nebo i kybergroomingu, odborník zdůraznil, že ten může mít následky opravdu dlouhodobé, někdy i celoživotní, a to jak na oběti, tak i na jejich okolí.

Motivace agresorů je podle slov experta ve většině případů pro vlastní uspokojení. Pachatelem, jak sám řekl, může být tedy kdokoli, může to být někdo s čistým trestním rejstříkem, ale i dávný kriminálník. Prevence je podle něho na lepší úrovni, než byla dříve, pořád je ale co zlepšovat a co se týče právního zakotvení, jsou podle něho nedostatky pouze v trestním právu procesním, kdy je největší problém doba, po kterou se čeká na informace k účtům pachatelů.

Na závěr odborník doporučil, aby uživatelé zejména přemýšleli nad tím, co na sociálních sítích dělají a komu důvěřují.

Závěr

Bezpečnostní rizika na sociálních sítích, jak můžeme soudit z celé práce, je opravdu fenomén dnešní doby, který není radno brát na lehkou váhu. Sociální sítě dnes neplní funkci, za jejímž účelem byly vytvořeny, a jsou spíše médiem, na kterém číhá spousta nástrah, i když nelze popřít, že lidem velmi usnadňují práci. Za nejnebezpečnější můžeme považovat sexting a kybergrooming, neboť mohou mít opravdu rozsáhlé a dlouhodobé následky. Ostatní zmíněné útoky však na úkor těchto nesmíme bagatelizovat. Každý útok zasahující do práv osob je velice vážnou záležitostí.

V této fázi práce je na místě verifikovat či falzifikovat v úvodu stanovené hypotézy. Co se tedy týče první hypotézy, tu můžeme s jistotou potvrdit. Jak jsme se dozvěděli v kapitole zabývající se situací v době COVIDU-19, útoků, a zejména vyhrožování a hoaxů, byl v této době rapidní nárůst. Také sám expert na danou problematiku uvedl, že kriminality páchané na internetu v době COVIDU-19 opravdu přibylo, a to zejména z důvodu opatření, která neumožňovala dostatečný sociální kontakt. Je třeba ale také zmínit, že to není způsobeno jen touto pandemii. Celkově v dnešní době ve společnosti převažuje komunikace online. Dnešní mladá generace si bez online světa nedokáže představit život a masivní většina je na mobilní telefony a jiné komunikační technologie skutečně upnuta.

Co se týče druhé hypotézy, tu můžeme taktéž potvrdil. Uvedl to jak odborník na danou problematiku, že nejohroženější skupinou a nejnáchylnější k tomu stát se oběťmi útoků na sociálních sítích, jsou děti do patnácti let. Zároveň i oběti zahrnuté do praktické časti této práce nám tento fakt potvrzují. Důležité je ale také zmínit, že lidé se často mylně domnívají, že se tato problematika rizik na sociálních sítích týká pouze dětí. Do ale například vztahových podvodů, se může dostat i kdejaký dospělý. Dostatečným důkazem je na stanici Netflix dokumentární film Podvodník z Tinderu, kde se oběťmi podvodu staly dospělé ženy.

Třetí hypotézu musíme vyvrátit, a to zejména na základě výpovědí respondentů prvních dvou rozhovorů z praktické části této práce, kteří se stali oběťmi kyberšikany především z toho důvodu, že příliš věřili blízkým osobám, které toho následně zneužily.

Nejdůležitější roli v oblasti této problematiky, jak již bylo zmíněno, hraje prevence. Ta by měla být cílena především na základní školy, zejména kvůli snižující se věkové hranici uživatelů sociálních sítí. Šlo by to realizovat například způsobem, jaký uváděl expert na danou problematiku, a to zavedením předmětu cíleného na toto téma nebo alespoň pořádáním pravidelných odborných přednášek, kde by se žáci dozvěděli, co jim hrozí, čemu se vyhnout, jak problém rozpoznat a jak ho v případě výskytu řešit.

Zároveň by ale mělo být posilováno všeobecné povědomí o těchto rizikách ve společnosti, například pomocí právě masových médií. Nástrojem pro to by se mohly stát i samotné oběti, kterým by nevadilo o jejich zkušenostech mluvit. Obě oběti z rozhovorů totiž uvedly, že se dostatečně poučily a od té doby jsou obezřetnější při zacházení a užívání sociálních sítí. Na tomto základě by mohly účinně apelovat na ostatní uživatele sociálních sítí. Tato prevence by měla být zaměřena zejména na upozorňování na to, co na internetu hrozí a jaké to může mít následky, a to zejména na základě skutečných příběhů. Také je důležité klást důraz na to, aby byl každý velice obezřetný, že by zásadně neměl věřit každému, na koho na sociální síti narazí, ale ani svým blízkým ve věcech přístupových údajů a intimní tématiky a měl by zvážit, které údaje o sobě zveřejní pro tisíce neznámých lidí, kteří jich mohou zneužít.

V úvodu stanovený cíl, kterým bylo zejména popsat základní pojmy vztahující se k problematice rizik na sociálních sítích, uvést některé jejich druhy a charakterizovat jednotlivé vybrané útoky na nich hrozící a s pomocí rozhovorů uskutečněných pro účely praktické části této práce formulovat závěry se zaměřením na možnosti prevence rizik na sociálních sítích, byl splněn.

Seznam použité literatury

Monografie

1. BLINKA, Lukáš. *Online závislosti: jednání jako droga? : online hry, sex a sociální sítě : diagnostika závislosti na internetu : prevence a léčba*. Praha: Grada, 2015. Psyché (Grada). ISBN 978-80-247-5311-9. 198 s.
2. ČERNÁ, Alena. *Kyberšikana: průvodce novým fenoménem*. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-247-4577-0. 150 s.
3. HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9. 217 s.
4. KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. 522 s.
5. KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3. 175 s.
6. KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: Grada Publishing, 2015. Průvodce (Grada). ISBN 978-80-247-5453-6. 183 s.
7. MARTÍNEK, Zdeněk. *Agresivita a kriminalita školní mládeže*. 2., aktualizované a rozšířené vydání. Praha: Grada, 2015. Pedagogika (Grada). ISBN 978-80-247-5309-6. 190 s.
8. NEŠPOR, Karel. *Návykové chování a závislost: současné poznatky a perspektivy léčby*. 5., rozšířené vydání. Praha: Portál, 2018. ISBN 978-80-262-1357-4. 255 s.
9. PETROWSKI, Thorsten. *Bezpečí na internetu: pro všechny*. Liberec: Dialog, 2014. Tajemství (Dialog). ISBN 978-80-7424-066-9. 243 s.
10. ŠEVČÍKOVÁ, Anna. *Děti a dospívající online: vybraná rizika používání internetu*. Praha: Grada, 2014. Psyché (Grada). ISBN 978-80-247-5010-1. 183 s.
11. VAŠUTOVÁ, Maria. *Proměny šikany ve světě nových médií*. Ostrava: Filozofická fakulta Ostravské univerzity v Ostravě, 2010. ISBN 978-80-7368-858-5. 225 s.

Zákonná úprava

1. Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) v posledním znění*
2. Zákon č. 40/2009 Sb., *trestní zákoník v posledním znění*

Webové stránky a elektronické zdroje

1. 66 stručných faktů o marketingu sociálních sítí. *Mytimi* [online]. [cit. 2022-01-23]. Dostupné z: https://www.mytimi.cz/66-strucnych-faktu-o-marketingu/
2. Bára. Sociální sítě – nevýhody. *JA IT* [online]. 27.2.2022 [cit. 2022-03-05]. Dostupné z: https://www.jait.cz/post/socialni-site-nevyhody
3. Co je kybergrooming?. *E-Bezpečí* [online]. 14.1.2019 [cit. 2022-02-09]. Dostupné z: https://www.e-bezpeci.cz/index.php/71-trivium/1421-co-je-kybergrooming
4. Hoax. *Internetem bezpečně* [online]. [cit. 2022-02-13]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/hoax/#1492560436505-570636f0-92f1412b-edf227c5-c79da29b-5208
5. JOHNSON, Joseph. Internet usage worldwide - statistics & facts. *Statista* [online]. 25.1.2022 [cit. 2022-03-05]. Dostupné z: https://www.statista.com/topics/1145/internet-usage-worldwide/#topicHeader__wrapper
6. KOPECKÝ, Kamil a René SZOTKOWSKI. *E-Bezpečí: Sexting jako riziková forma komunikace (průvodce studiem)* [online]. Olomouc, 2018 [cit. 2022-02-09]. Dostupné z: https://www.pdf.upol.cz/fileadmin/userdata/PdF/VaV/2018/odborne_seminare/E-Bezpeci_-_Sexting_jako_rizikova_forma_komunikace.pdf
7. KOS, Adam. Meta: Vše, co byste měli vědět o přejmenovaném Facebooku. *Jablíčkář* [online]. 29.10.2021 [cit. 2022-02-20]. Dostupné z: https://jablickar.cz/meta/
8. KYBERGROOMING A KYBERSTALKING: Metodický materiál pro pedagogické pracovníky. *Národní centrum bezpečnějšího internetu* [online]. PROJEKT ŠKOLA BEZPEČNĚ ONLINE, 2012 [cit. 2022-02-09]. Dostupné z: https://www.ncbi.cz/projekty/ukoncene-projekty/op-vk/opvk-skola-bezpecne-online.html

9. Kyberkriminalita. *Policie České republiky* [online]. [cit. 2022-02-06]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx
10. LINKEDIN: Sociální síť LinkedIn. *Sítě v hrsti* [online]. [cit. 2022-01-23]. Dostupné z: https://sitevhrsti.cz/socialni-site/linkedin/
11. Most popular social media platforms in the Czech Republic in 2021, by posting frequency. *Statista* [online]. Statista Research Department, 11.1.2022 [cit. 2022-02-20]. Dostupné z: https://www.statista.com/statistics/1281528/czechia-social-media-platforms-by-posting-frequency/
12. Muž obviněný z vyhrožování Babišovi mu zaslal omluvu. Odpustil jsem mu, říká premiér. *Aktuálně.cz* [online]. Česká tisková kancelář, 15.4.2021 [cit. 2022-01-02]. Dostupné z: https://zpravy.aktualne.cz/domaci/muz-obvineny-z-vyhrozovani-babisovi-mu-zaslal-omluvu/r~f4da99409dda11ebb9860cc47ab5f122/
13. Number of monthly active mobile social media users in Europe as of January 2021, by country. *Statista* [online]. Statista Research Department, 28.1.2022 [cit. 2022-02-20]. Dostupné z: https://www.statista.com/statistics/299496/active-mobile-social-media-users-in-european-countries/
14. OTEVŘENÁ VĚDA, Odborný garant dílu - doc. Ing. Pavel Peterka, Ph.D. NEZkreslená věda: pátá série vzdělávacího cyklu Akademie věd České republiky.: JAK FUNGUJE INTERNET – NEZkreslená věda V. *YouTube* [online]. 4. 5. 2020, 9:48 minut. [cit. 2021-12-15]. Dostupné z: https://www.youtube.com/watch?v=L05HGoaDkRo&ab_channel=Otev%C5%99en%C3%A1v%C4%9Bda
15. PAVLAS MARTANOVÁ, Veronika. O PRIMÁRNÍ PREVENCI RIZIKOVÉHO CHOVÁNÍ. *Národní ústav pro vzdělávání* [online]. květen 2014 [cit. 2022-03-01]. Dostupné z: https://www.nuv.cz/t/co-je-skolska-primarni-prevence-rizikoveho-chovani
16. PAVLÍČEK, Michal. Instagram slaví 10 let. Aktivně ho používá miliarda uživatelů po celém světě. *Mobilnet* [online]. 6.10.2020 [cit. 2022-01-23]. Dostupné z: https://mobilenet.cz/clanky/instagram-slavi-10-let-aktivne-ho-pouziva-miliarda-uzivatelu-po-celem-svete-41860

17. Policie ČR. *Twitter* [online]. 3.12.2021 [cit. 2022-01-02]. Dostupné z: https://twitter.com/PolicieCZ/status/1466730134891909125
18. Přehled seznamovacích kategorií. *Seznamka.cz* [online]. [cit. 2022-01-23]. Dostupné z: https://www.seznamka.cz/inzeraty/kategorie.aspx
19. Reklama. *Líbím se ti* [online]. [cit. 2022-01-23]. Dostupné z: http://napoveda.libimseti.cz/reklama/
20. RODRIGUEZ, Cecilia. Třetina lidstva nikdy nespatřila internet. Proč jsou tři miliardy lidí stále offline?. *Forbes* [online]. 27.12.2021 [cit. 2022-03-03]. Dostupné z: https://forbes.cz/tretina-svetove-populace-nikdy-nespatrila-internet-proc-jsou-skoro-tri-miliardy-lidi-stale-offline/
21. Sociální sítě: Co je sociální síť. *Nebojte se Internetu* [online]. cz.nic [cit. 2022-02-11]. Dostupné z: https://www.nebojteseinternetu.cz/page/3396/socialni-site/
22. Sociální sítě: Dělení sociálních sítí. *Nebojte se Internetu* [online]. cz.nic [cit. 2022-02-11]. Dostupné z: https://www.nebojteseinternetu.cz/page/3396/socialni-site/
23. Sociální sítě: Znaky sociálních sítí. *Nebojte se Internetu* [online]. cz.nic [cit. 2022-02-11]. Dostupné z: https://www.nebojteseinternetu.cz/page/3396/socialni-site/
24. Statistiky využití sociálních sítí: Kolik lidí používá sociální média v roce 2021?: KOLIK LIDÍ POUŽÍVÁ SOCIÁLNÍ SÍTĚ?. *Ler.studio* [online]. 22.6.2021 [cit. 2022-01-23]. Dostupné z: https://lerstudio.cz/statistiky-vyuziti-socialnich-siti-kolik-lidi-pouziva-socialni-media-v-roce-2021
25. Statistiky využití sociálních sítí: Kolik lidí používá sociální média v roce 2021?: STATISTIKY VYUŽITÍ SOCIÁLNÍCH MÉDIÍ. *Ler.studio* [online]. 22.6.2021 [cit. 2022-01-23]. Dostupné z: https://lerstudio.cz/statistiky-vyuziti-socialnich-siti-kolik-lidi-pouziva-socialni-media-v-roce-2021
26. VRCHOTA, Matouš. Co je to metaverse? A proč v něm Facebook alias Meta vidí svou budoucnost?. *Inteligentní svět* [online]. 2.11.2021 [cit. 2022-02-20]. Dostupné z: https://inteligentnisvet.cz/clanky/co-je-to-metaverse-proc-je-to-budoucnost-firmy-facebook-meta
27. Využívání informačních a komunikačních technologií v domácnostech a mezi osobami - 2021: Počítače a internet v domácnostech - Tab. 1.4 Domácnosti v

ČR s internetem – vývoj v čase. *Český statistický úřad* [online]. 2021 [cit. 2021-12-15]. Dostupné z: https://www.czso.cz/csu/czso/1-pocitace-a-internet-v-domacnostech-f1de7iri8s

28. Využívání informačních a komunikačních technologií v domácnostech a mezi osobami - 2021: 7. Sociální sítě - Tab. 7.2 Osoby v ČR používající sociální sítě – vývoj v čase. *Český statistický úřad* [online]. 23.11.2021 [cit. 2022-01-02]. Dostupné z: https://www.czso.cz/csu/czso/7-socialnisite

Seznam příloh

Příloha číslo 1 – Informovaný souhlas pro oběti

Příloha číslo 2 – Informovaný souhlas pro experta

Přílohy práce

Příloha číslo 1 – Informovaný souhlas pro oběti

Informovaný souhlas pro oběti

Fakulta bezpečnostního managementu Policejní akademie České republiky v Praze

Jméno zpracovatele: Tereza Kisby

Já níže podepsaný(á) souhlasím s mou účastí ve výzkumu k bakalářské práci na téma „Bezpečnostní rizika na sociálních sítích“ a se zpracováním získaných informací v této práci.

Byl(a) jsem podrobně informován(a) o cíli studie, o jejích postupech a podmínkách, a o tom, co se ode mě očekává.

Porozuměl(a) jsem tomu, že mohu z výzkumu odstoupit do 5 dnů od poskytnutí informací. Moje účast ve studii je dobrovolná.

Byl(a) jsem srozuměna s tím, že výsledky jsou zcela anonymní a budou použity výhradně k interpretaci výsledků v této bakalářské práci.

Jelikož se jedná o rozhovor, souhlasím s jeho nahráváním, následným přepisem a jeho analýzou.

Jsem srozuměn(a) s tím, že pokud se v rozhovoru vyskytne pro mě citlivá otázka, mohu odmítnout odpovědět.

V: …… Dne: ……

Podpis: ……

Příloha číslo 2 – Informovaný souhlas pro experta

Informovaný souhlas pro experta

Fakulta bezpečnostního managementu Policejní akademie České republiky v Praze

Jméno zpracovatele: Tereza Kisby

Já níže podepsaný(á) souhlasím s mou účastí ve výzkumu k bakalářské práci na téma „Bezpečnostní rizika na sociálních sítích“ a se zpracováním získaných informací v této práci.

Byl(a) jsem podrobně informován(a) o cíli studie, o jejích postupech a podmínkách, a o tom, co se ode mě očekává.

Porozuměl(a) jsem tomu, že moje účast ve studii je dobrovolná.

Byl(a) jsem srozuměn(a) s tím, že výsledky budou interpretovány pod mým jménem a výhradně v této bakalářské práci.

Jelikož se jedná o rozhovor, souhlasím s jeho nahráváním, následným přepisem a jeho analýzou.

V: …… Dne: ……

Podpis: ……