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

Radek Sokola

PRAHA

2024

Čestné prohlášení:

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

V Praze, dne 15. března 2024

……

Radek Sokola

Poděkování

Poděkování bych chtěl věnovat vedoucímu práce Mgr. Josefu Dubskému za odborné vedení této práce. Velké díky dále patří mému kolegovi z řad Policie České republiky, a to za odborné připomínky z pohledu specialisty prevence.

Anotace

Tato bakalářská práce se zabývá bezpečnostními riziky, které mohou hrozit v souvislosti s užíváním sociálních sítí. V teoretické části jsou uvedeny základní pojmy, které jsou s tímto tématem neodmyslitelně spjaty, podrobný popis sociálních sítí, představení nejrozšířenějších rizik, nejohroženější skupiny naší populace a prevence před jednotlivými riziky a možné právní důsledky, které lze z popsaných rizik vyvodit. Praktická část této práce je zaměřena na reálné útoky v online prostředí, které jsou zprostředkovány formou kazuistik, přičemž tato část práce je zakončena rozhovorem se specialistou prevence z řad Policie ČR, který k práci doplní své odborné připomínky a zkušenosti.

Klíčová slova internet * online prostředí * rizika a hrozby * kyberšikana * zneužití osobních údajů * dezinformace * online predátoři * závislost * prevence

Annotation

This bachelor's thesis deals with security risks that may arise in connection with the use of social networks. In the theoretical part, the basic concepts that are inherently connected with this topic are presented, a detailed description of social networks, an introduction of the most widespread risks, the most endangered groups of our population and prevention of individual risks and possible legal consequences that can be derived from the described risks. The practical part of this work is focused on real attacks in the online environment, which are mediated in the form of case studies, while this part of the work is concluded with an interview with a prevention specialist from the Police of the Czech Republic, who will add his professional comments and experience to the work.

Keywords internet * online environment * risks and threats * cyberbullying * misuse of personal data * misinformation * online predators * addiction * prevention

Obsah

Úvod **7**

I. TEORETICKÁ ČÁST **9**

1 Základní pojmy **9**

1.1 Internet a kyberprostor 9

1.1.1 Historie internetu 11

1.1.2 Zásadní vliv internetu na dnešní dobu 13

1.2 Kyberidentita a digitální stopa 15

1.3 Sociální sítě 17

1.3.1 Historie sociálních sítí 20

1.3.2 Druhy sociálních sítí 21

1.3.3 Nejznámější sociální sítě v ČR 22

2 Bezpečnost a možná rizika na sociálních sítích **24**

2.1 Kyberšikana 25

2.1.1 Prostředky k realizaci kyberšikany 25

2.1.2 Formy kyberšikany 26

2.2 Zneužití osobních údajů 28

2.3 Dezinformace, fake news a hoaxy 30

2.4 Online predátoři 31

2.4.1 Kybergrooming 32

2.5 Závislost na sociálních mediích 33

3 Nejzranitelnější skupiny uživatelů a prevence jednotlivých bezpečnostních rizik **36**

4 Trestná činnost páchána ve virtuálním prostředí **41**

II. Praktická část **43**

5 Kazuistiky rizik na sociálních sítích **43**

5.1 Kazuistika č. 1 44

5.2 Kazuistika č. 2 45
5.3 Kazuistika č. 3 46
5.4 Kazuistika č. 4 47
5.5 Kazuistika č. 5 49
6 Správný postup a doporučení prevence 51
6.1 Kyberšikana 51
6.2 Online predátoři 52
6.3 Šíření dezinformací 54
6.4 Zneužití osobních údajů 55
6.5 Závislost na sociálních médiích 57
6.6 Doplňující otázky 58
Závěr 60
Seznam použité literatury 62

Úvod

V současné digitální éře se naše společnost stále více propojuje prostřednictvím sociálních sítí. Tyto platformy se staly virtuálními místy pro sdílení radostí, názorů, informací a poskytují efektivní, snadno dostupnou a rychlou možnost propojení s kýmkoliv, na jakémkoliv místě na naší planetě. Navzdory těmto kladným aspektům, využívání sociálních sítí s sebou přináší velkou řadu bezpečnostních rizik, na které nesmíme zapomínat. Téma bezpečnostních rizik na sociálních sítích se stává stále aktuálnějším a důležitějším, neboť využívání sítí po nás na internet zanechává „digitální stopy“, které se proplétají s naším každodenním životem. Sociální sítě nám tak otevírají dveře do světa, kde kybernetická bezpečnost není pouze technologickou otázkou, ale také otázkou ochrany našich osobních životů.

Z tohoto důvodu je velmi důležité informovat každého, kdo tyto sítě používá, o možných hrozbách v tomto „digitálním světě“.

Cílem této práce je pomocí deskriptivní a analyticko-syntetické metody vymezit podstaty vybraných útoků a hrozeb vznikajících na sociálních sítích, na jejichž základě budou formulovány závěry se zaměřením na prevenci.

Práce je rozdělena na dvě části, a to na část teoretickou a část praktickou. Teoretická část této práce obsahuje čtyři kapitoly. V první kapitole bylo zapotřebí definovat základní pojmy, které neodmyslitelně souvisejí s riziky na sociálních sítích. Jedná se o pojmy internet a kyberprostor, kyberidentita a digitální stopa a sociální sítě. Druhá kapitola je jednou ze stěžejních kapitol této práce a má za úkol čtenáři co nejvíce přiblížit nejrozšířenější hrozby, které se na sociálních sítích objevují. Těmito hrozbami jsou kyberšikana, zneužití osobních údajů, dezinformace, fake news a hoaxy, online predátoři a závislost na sociálních médiích. Třetí kapitola pojednává o nejzranitelnějších uživatelích a prevenci v závislosti na jednotlivé hrozby. Poslední kapitola teoretické části této práce je zaměřena na možnou protiprávní činnost agresorů v online prostředí.

Praktická část této práce je tvořena pěti kazuistikami, kdy každá doplňuje jednotlivé hrozby z teoretické části o reálné zkušenosti obětí.

Následující část praktické části je zaměřena na rozhovor se specialistou prevence z řad Policie České republiky, který jednotlivé kazuistiky doplní o odborný názor na správný postup obětí a uvede preventivní opatření ke každé vybrané hrozbě.

V závěru této práce jsou formulovány možnosti, jakými by bylo možné zlepšit prevenci a eliminovat tak výskyt rizik, a to zejména v oblasti informovanosti uživatelů a využití nových technologií.

I. TEORETICKÁ ČÁST

1 Základní pojmy

Tato kapitola definuje základní pojmy, které se neodmyslitelně vztahují k problematice rizik, hrozících v souvislosti s používáním sociálních sítích, a to zejména proto, aby se čtenář v rámci následujících textů, v těchto pojmech orientoval. Jedná se o pojmy Internet a kyberprostor, kyberidentita a digitální stopa a sociální sítě.

1.1 Internet a kyberprostor

Vzhledem k tomu, že tato práce se zabývá bezpečnostními riziky na sociálních sítích a tyto sítě vznikly jenom díky Internetu, je zapotřebí čtenáři přiblížit, co to Internet je. Pro snadnější orientaci vývoje a vzniku sociálních sítí je rovněž důležité objasnění dějin samotného Internetu.

Slovo internet je zkratkou pro anglický název interconnected networks, který ve volném překladu znamená propojené sítě. Jde vlastně o globální síť propojující mnoho počítačů a dalších zařízení po celém světě, přičemž tato zařízení spolu komunikují, sdílí informace a přenáší mezi sebou data na základě stanovených pravidel, které jsou vytyčeny skupinou protokolů „TCP/IP (Transmission control protocol – Protokol řízení přenosu a Internet protocol – Internetový protokol).

Pro zjednodušení výše uvedeného popisu si lze internet představit jako pavučinu, kdy vlákno této pavučiny je jakýmsi spojovacím prvkem a uzly vytvořené propojením těchto vláken jsou jednotlivými uživateli, přičemž propojením mezi sebou vytváří síť.[1]

Pojem internet je rovněž popisován v nepřeberném množství odborné literatury. PhDr. Jan Šmahaj, Ph.D. ve své knize s názvem Kyberšikana jako společenský problém popisuje internet následovně: „*Internet (INTERconected computer NETwork) je globální síť, která propojuje lokální počítačové sítě a zároveň poskytuje různé služby (např. osobní a komerční webové stránky, sociální sítě,*

[1] TURBONET. Co je to internet a jak vlastně funguje? [online]. [cit. 2024-02-29]. Dostupné z: https://turbonet.cz/odpovedi-internetove-pripojeni/co-je-to-internet-a-jak-vlastne-funguje

globální vyhledávače). Zahrnuje v sobě přístup k informacím písemného, obrazového i audio obsahu.“[2]

Dalším autorem, který skrze svou knihu s názvem CyberCrime sdílí své pojetí internetu, je JUDr. Jan Kolouch, Ph. D., který uvádí následující: *„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.“*[3]

S pojmem internet se neodmyslitelně pojí další výraz, kterým je kyberprostor. Veřejnost se často domnívá, že tyto dva pojmy mají totožný význam. Nicméně autoři odborné literatury se shodují na tvrzení, že mezi internetem a kyberprostorem existují určité odlišnosti.

Pierre Lévy, francouzský profesor na katedře hypermédií Univerzity Paris-St. Denis, ve své knize s názvem Kyberkultura definuje kyberprostor jako: „*Nové komunikační prostředí, které povstává z celosvětového propojení počítačů.“*[4]

Jasnější pojetí kyberprostoru předkládá autorka Lenka Hulanová ve své knize s názvem Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality, kde objasňuje zásadní rozdíl mezi internetem a kyberprostorem: *„Kyberprostor je prostor, který se nám otevírá ve chvíli, kdy pomocí internetových sítí vstupujeme do on-line prostředí.“*[5]

Tímto je tedy zřejmé, že kyberprostor a internet jsou dva odlišné výrazy, kdy každý z nich vykazuje odlišné pojetí v on-line prostředí a každý z nich má v tomto prostředí své opodstatněné místo.

---

[2] ŠMAHAJ, Jan. Kyberšikana jako společenský problém: Cyberbullying as a social problem. Olomouc: Univerzita Palackého v Olomouci, 2014. ISBN 978-80-244-4227-3. s. 16.
[3] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 43.
[4] LÉVY, Pierre. Kyberkultura: zpráva pro Radu Evropy v rámci projektu "Nové technologie: kulturní spolupráce a komunikace". V Praze: Karolinum, 2000. ISBN 80-246-0109-5. s. 15.
[5] HULANOVÁ, Lenka. Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality. Praha: Triton, 2012. ISBN 978-80-7387-545-9. s. 27.

1.1.1 Historie internetu

Internet je nepochybně jedním z největších vynálezů lidstva. Historie internetu je úzce spjata se vznikem počítačů (po roce 1945). Vzhledem k tomu, že bylo zapotřebí, aby tato zařízení mohla spolu vzájemně komunikovat, dala tak tato situace vzniknout **počítačovým sítím**.

Dle dostupných informací lze za prvotní a významný impuls pro počátky vzniku internetu považovat vypuštění sovětské družice Sputnik 1 v roce 1957. V této době probíhala mezi USA a SSSR již od roku 1947 „studená válka“ a právě ono vypuštění družice ze strany SSSR bylo pro USA drsným ukazatelem, jak moc zaostávají v oblasti kosmických technologií, které byly úzce spjaté i s vojenskou technologií, což mohlo pro USA zvěstovat nepříznivý vývoj uváděného konfliktu. Vzhledem k tomu, že zde byla dána hrozba zničení komunikační infrastruktury za použití jaderných zbraní, reagovaly Spojené státy na tuto hrozbu zadáním úkolu agentuře ARPA (Dnes DARPA - Defense Advanced Research Projects Agency, přeloženo jako Agentura ministerstva obrany pro pokročilé výzkumné projekty). Tato agentura měla vytvořit komunikační síť pro počítače, jejíž provoz by nevyžadoval žádné řídící uzly (v té době pro komunikaci používané telefonní ústředny jako zmiňované řídící uzly) a místo toho by bylo řízení celé sítě decentralizováno. Díky decentralizaci řízení této sítě by mohla dále fungovat, i kdyby z jakéhokoliv důvodu došlo k výpadku některé z jejích částí. Dnes je tato síť pojmenována Internet.[6]

Vývoj dějin internetu by se dal shrnout do šesti zásadních milníků.

1. Před ARPANET: Koncept propojení (60. léta):

V 60. letech 20. století se začaly zkoumat a vyvíjet možnosti komunikace mezi fyzicky oddělenými systémy. Tyto výzkumy vedly k vývoji modelu „přepojování paketů“ v digitální síti (odesílaná data cestují po menších částech a celek

[6] Přispěvatelé Wikipedie, Dějiny internetu [online], Wikipedie: Otevřená encyklopedie, c2024, Datum poslední revize 9. 01. 2024, 09:33 UTC, [citováno 29. 02. 2024]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=D%C4%9Bjiny_internetu&oldid=23545849

sestavuje až příjemce). Projekt v laboratoři pro výzkum na poli balistického výzkumu (RAND) představil jeden z prvních konceptů takového systému.[7]

2. ARPANET: První krok (1969):

Výše uváděné výzkumy vedly k tomu, že v roce 1968 se začalo naplno hovořit o počítačových komunikačních sítích, přičemž přenos dat mezi počítači měl být umožněn díky jejich rozdělení do malých bloků (paketů), tak jak předjímaly výzkumy z laboratoří RAND. V roce 1969 byla spuštěna historicky první počítačová síť pod názvem ARPANET (Advance Research Projects Agency Network – v překladu síť Agentury pro pokročilé výzkumné projekty) pod záštitou amerického ministerstva obrany. V počátcích tato síť propojila pouze 4 výzkumná centra v západní části Spojených států. V roce 1970 se již tato síť propojila i s východním pobřežím USA. Projekt ARPANET se tak stal prvním krokem k vytvoření globální sítě.[8]

3. Protokoly TCP/IP (70. a 80. léta):

V roce 1973 došlo k úspěšnému přenosu počítačových souborů mezi desítkami počítačů, které byly rozmístěny na různých místech v USA. Tento přenos byl umožněn na základě protokolu FTP (File Transfer Protocol), čímž byl položen opravdový základ moderní internetové sítě.

Rok 1974 přinesl nový název pro vznikající globální síť – internet. Poprvé tento termín byl použit při zformulování dvou základních principů fungování sítě – internetový protokol (Internet Protocol - IP) a protokol řízení přenosu (Transmission Control Protocol - TCP). Zařízení, které zvládlo využít kombinaci těchto dvou metod, tedy TCP/IP, mělo být schopné komunikovat s jakýmkoliv zařízením na světě. Celé to fungovalo tak, že internetový protokol zajistil propojení vzdálených zařízení díky dvěma unikátním IP adresám, zatímco protokol řízení přenosu (TCP) zajišťoval korektní způsob odeslání datových paketů.

[7] CZ.NIC. Jak na internet: Historie internetu [online]. [cit. 2024-02-29]. Dostupné z: https://www.jaknainternet.cz/page/1205/historie-internetu/
[8] Tamtéž

V tuto dobu byl Internet stále vyhrazen pouze pro akademickou komunitu. Uváděné protokoly jsou však nosným pilířem Internetu i v dnešní době.[9]

4. World Wide Web (1989-1991):

Revolucí, která zapříčinila pozdější globální rozšíření Internetu, byl vznik World Wide Web – neboli WWW, kterou vytvořil Tim Berners-Lee v roce 1989. Toto vedlo k zavedení prvního webového serveru v roce 1991, čímž byly otevřeny dveře pro vznik a prohlížení webových stránek, což výrazně posílilo dostupnost internetu.[10]

5. Růst komerčního využití (90. léta):

V průběhu 90. let 20. století se internet stal komerčně dostupným pro širší veřejnost. Nástup webového prohlížeče Netscape (předchůdce dnes dobře známých prohlížečů, jako jsou Internet Explorer, Google Chrome a další) v roce 1994 zapříčinil počátek masového užívání internetu a začal rovněž podporovat rozvoj internetového obchodu.[11]

6. 21. Století: Globalizace a sociální média:

V průběhu 21. století internet překročil národní hranice, čímž se stal klíčovou součástí globální společnosti. Sociální média, cloudové technologie a různé další inovace změnily způsob, jakým dnes lidé komunikují, pracují, nakupují a získávají informace. Navzdory uvedeným inovacím se však na internetu masivně rozšířila rovněž kybernetická kriminalita a různé další hrozby napříč všemi uživateli ve všech věkových kategoriích. [12]

1.1.2 Zásadní vliv internetu na dnešní dobu

V dnešní době je internet nejen nedílnou součástí našeho každodenního života, ale stal se i klíčovým prvkem pro globální komunikaci, informační výměnu, vzdělávání, a obchodní aktivity. Tato kapitola se zaměří na aktuální rozsah a

[9] CZ.NIC. Jak na internet: Historie internetu [online]. [cit. 2024-02-29]. Dostupné z: https://www.jaknainternet.cz/page/1205/historie-internetu/
[10] Tamtéž
[11] NEJPRIPOJENI. Z historie internetu [online]. [cit. 2024-02-29]. Dostupné z: https://nejpripojeni.cz/clanky/z-historie-internetu/
[12] Přispěvatelé Wikipedie, Globalizace [online], Wikipedie: Otevřená encyklopedie, c2024, Datum poslední revize 20. 02. 2024, 10:27 UTC, [citováno 29. 02. 2024] https://cs.wikipedia.org/w/index.php?title=Globalizace&oldid=23677425

význam využití internetu, zkoumajíc, jak tento fenomén ovlivňuje různé sféry našeho života.

Dnešní internetová doba je charakterizována zejména univerzálním přístupem k internetu. Stále více lidí po celém světě má možnost připojit se k internetu, což znamená, že tato technologická síť není omezena na konkrétní geografické oblasti nebo sociální skupiny, ale je dostupná téměř každému. Přístup k informacím, komunikaci a online zdrojům se tak stává klíčovým faktorem pro každodenní život.

1. Komunikace

Internet má zásadní vliv na mezikulturní komunikaci. Díky internetu spolu mohou komunikovat lidé z různých koutů světa, sdílet své názory a tím i poznávat odlišné kultury, což může vést k většímu vzájemnému porozumění. Rovněž vytváří prostor pro virtuální společenství, kde neexistují žádné hranice. Internet se tak nepopiratelně stává jedním z nástrojů pro globalizaci, kde informace, nápady a aktuální světové dění volně proudí napříč národními hranicemi. V dnešní době není internet pouze technologickým nástrojem, ale též klíčovým prvkem pro formování globálních vztahů a kultury. Jde ruku v ruce s procesem globalizace, přinášející příležitosti, ale také vyzývající nás k řešení otázek spojených s hrozbami, rovností a etikou.[13]

2. Ekonomika

Internet rovněž přinesl revoluční změnu v oblasti podnikání. Dnešní podoba internetového prostředí ovlivňuje způsob, jakým firmy operují, komunikují a obchodují, stejně tak, jakým způsobem lidé zboží vyhledávají a nakupují ho. Od vzniku e-commerce (internetový obchod), po rozšíření online marketingu, se tak internet stal klíčovým prvkem v obchodním ekosystému.

[13] ŠANCE DĚTEM. Jak internet ovlivňuje život dětí a dospívajících? [online]. [cit. 2024-02-29]. Dostupné z: https://sancedetem.cz/jak-internet-ovlivnuje-zivot-deti-dospivajicich

V oblasti ekonomiky se internet stal klíčovým prvkem pro transformaci obchodního prostředí, neboť firmy musí aktivně reagovat na digitální trendy a využívat internet k inovaci a zlepšení svých podnikatelských procesů.[14]

3. Vzdělávání

Internet rovněž zásadně změnil vzdělávací prostředí. Nehledě na to, že jsou lidem po pár kliknutí přístupné jakékoli informace k jakémukoliv tématu, existují rovněž různé online výukové materiály a interaktivní kurzy, čímž se vytváří daleko flexibilnější přístup ke vzdělání.

Online knihovny, vědecké články a digitální archivy přispívají k rozvoji výzkumných kapacit a zvyšují úroveň vzdělávání.

Online zdělávání rovněž dalo vzniknout konceptům, jako jsou e-learning a distanční vzdělávání díky, kterým studenti mohou studovat bez ohledu na geografickou vzdálenost, což umožňuje eliminaci absence školních zařízení v místě bydliště studentů.

Co se týče vzdělávání, tak je nutné poznamenat, že internet není pouze pasivním prostředím pro získávání informací, ale stává se aktivním partnerem ve vzdělávacím procesu, umožňujícím inovace a přizpůsobení vzdělávání potřebám dnešní moderní doby.[15]

1.2 Kyberidentita a digitální stopa

Tato kapitola má za úkol zvýšit povědomí o důležitosti digitální stopy a jejím vlivu na digitální identitu (kyberidentitu) a seznámit čtenáře s významem těchto slov, neboť v rámci bezpečnosti na internetu a sociálních sítích hrají digitální stopa a kyberidentita významnou roli především v oblasti soukromí a správy osobních informací v online prostoru.

[14] DENÍK VEKTOR. Informační technologie, umělá inteligence a ekonomika [online]. [cit. 2024-02-29]. Dostupné z: https://www.denikvektor.cz/ai/informacni-technologie-umela-inteligence-a-ekonomika-2373.html

[15] ESTUDOVNA. Vzdělávání po internetu [online]. [cit. 2024-02-29]. Dostupné z: https://www.estudovna.cz/cz/co-je-e-learning-vzdelavani-po-internetu95.html

Je důležité si uvědomit, že v éře, kdy digitalizace pronikla do našich každodenních životů, máme nejen fyzickou identitu, ale také její kybernetický protějšek – kyberidentitu.

Kyberidentita představuje digitální podobu jednotlivce v online prostoru. Od sociálních sítí, přes online nákupy, až po sledování videí – jakákoliv internetová interakce zanechává digitální stopu a tím přispívá k formování naší kyberidentity, která často zahrnuje informace o uživateli, jako jsou jméno, fotografie, příspěvky na sociálních sítích (tedy různé informace z osobního života) a online komunikace. [16]

S pojmem kyberidentita se neodmyslitelně pojí digitální stopa, neboť ucelený soubor digitálních stop, které každý jednotlivec zanechává při svých aktivitách na internetu, vytváří kyberidentitu daného jedince. Digitální stopa je tvořena veškerou naši online činností (online vyhledávání, aktivitami na sociálních sítích, e-mailovou komunikací apod.). Je to virtuální otisk, který odhaluje naše chování a interakce v online prostoru. Jan Kolouch ve své knize s názvem CyberCrime uvádí k digitální stopě, že: „*Za digitální stopu je možné označit jakákoli data či informace přenesená, vytvořená, uložená či modifikovaná za použití počítačového systému*“ [17]

Nejčastější aktivity, které zanechávají digitální stopy a formují kyberidentitu

Sociální média: Vyváření profilů na sociálních sítích je jedním z klíčových prvků formování kyberidentity. Obsah, který zde sdílíme a interakce s ostatními uživateli tvoří základ naší virtuální podoby.

Online komunikace: Každý e-mail, komentář nebo diskuzní příspěvek přispívá k tomu, jak nás vnímají ostatní uživatelé z různých online komunit a zároveň po nás zanechává snadno dohledatelnou digitální stopu.

Online aktivity: Sledování videí, čtení zpráv, online hry. Veškeré tyto činnosti po nás zanechávají digitální stopu a formují naší kyberidentitu.

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

Online nákupy: Nákupy na internetu zanechávají digitální stopu v podobě historie nákupů a osobních preferencí, na jejichž základě mohou vznikat reklamy cílené na jednotlivé uživatele.

Vyhledávání: Každé vyhledávání na internetu je zaznamenáno a tvoří část naší digitální stopy.[18]

Správa digitální stopy a bezpečnost

Stále více internetových medií nabízí svým uživatelům možnosti, jak spravovat svou digitální stopu, a to zejména pomocí „nastavení soukromí a správy online účtů“. Nicméně je důležité si uvědomit, že každý z nás má zodpovědnost za to, jaká stopa zůstane za ním. Nastavení soukromí a osobní uvědomění spolu s adekvátní obezřetností jsou v tomto případě klíčové.[19]

Závěrem této kapitoly lze říci, že naše online aktivity mohou mít dlouhodobý dopad na naši kyberidentitu a tedy každý jednotlivec je zodpovědný za to, jak sám sebe v digitálním prostředí prezentuje.

Kyberidentita může být také cílem některých útoků, kterými jsou například phishing či krádež identity. Útokům, které souvisí s používáním sociálních sítí (tedy i s digitální stopou a kyberidentitou) se v rámci této práce bude zabývat samostatná kapitola.

1.3 Sociální sítě

Sociální sítě jsou online platformy, které umožňují uživatelům vytvářet profily, sdílet obsah, komunikovat s ostatními uživateli a budovat virtuální komunity. Sociální sítě jsou samy o sobě jakýmsi digitálním prostředím, kde se prolíná virtuální a reálný svět, který svým uživatelům umožňuje sdílet informace, navazovat spojení a interagovat napříč geografickými hranicemi.[20]

[18] INTERNETEM BEZPEČNĚ. Digitální stopa [online]. [cit. 2024-02-29]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/
[19] Tamtéž
[20] KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

Autoři Martin Kožíšek a Václav Písecký ve své knize Bezpečně n@ internetu, definují sociální sítě následovně: *„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]

Pro účely této práce bych však vybral zejména definici, která se objevila v publikaci s názvem Bezpečnost v online prostředí. Jedním z autorů této publikace je Mgr. Radek Karchňák, který je klinickým psychologem a k publikaci přispěl zejména informacemi o psychologických dopadech kybernetické kriminality na její oběti.

Druhým autorem, který se na publikaci podílel je Roman Kohout, který je příslušníkem Policie ČR, specializuje se na vyšetřování kybernetické trestné činnosti a také je zakladatelem projektu „Internetem bezpečně“. V již zmíněné publikaci definují oba výše jmenovaní sociální sítě jako: *„online službu, která na základě registrace umožní vytvořit profil uživatele, pod kterým lze tuto službu využívat zejména ke komunikaci, sdílení informací, fotografií, videa atd. s dalšími registrovanými uživateli.“*[22]

Sociální sítě se také zakládají na určitých klíčových rysech, které definují tuto formu online interakce. Těmito rysy jsou:

- *„Vytváření uživatelských profilů“* - každý uživatel sociální sítě si vytváří svůj vlastní uživatelský profil obsahující informace o sobě. Tyto profily zahrnují fotografie, osobní údaje, zájmy a další informace, které tvoří kyberidentitu jednotlivce.
- *„Vzájemné propojení“* - vzájemné propojení je klíčovým prvkem sociálních sítí. Uživatelé mohou "přidat" nebo "sledovat" své přátele a známé. Tímto způsobem se vytvářejí tzv. „digitální sítě spojení“.
- *„Novinky a Feed“* – jedním z hlavních prvků většiny sociálních sítí je sekce novinek nebo „feed“, kde uživatelé vidí příspěvky svých přátel a

[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.
[22] KOHOUT, Roman a KARCHŇÁK, Radek. Bezpečnost v online prostředí. Karlovy Vary: Biblio Karlovy Vary, 2016. ISBN 978-80-260-9543-9. s. 40.

sledovaných osob. Tato nepřetržitá aktualizace zobrazuje obsah, který je relevantní pro daného uživatele pomocí sledování zanechané digitální stopy (např. po shlédnutí vtipného videa se nám budou více zobrazovat vtipná videa v sekci novinek).

- *„Sdílení obsahu“* - uživatelé mohou na sociálních sítích sdílet různé formy obsahu, včetně textu, fotografií, videí, odkazů a dalších multimediálních prvků. Tato schopnost sdílet umožňuje uživatelům vyjádřit své myšlenky a zážitky a také sympatizovat s podobně smýšlejícími uživateli.
- *„Interakce a komentáře“* - sociální sítě poskytují prostor pro interakci mezi uživateli. Kromě vyjádření kladného vztahu k příspěvku (označením „To se mi líbí“) mohou uživatelé reagovat komentáři, což umožňuje diskuzi a zapojení se do sociálních komunit.
- *„Soukromí a nastavení bezpečnosti“* – známé a nejvíce využívané sociální sítě umožňují uživatelům nastavovat stupně soukromí. Uživatelé tak mohou určit, kdo může vidět jejich obsah, a kdo s nimi může navázat spojení.
- *„Skupiny a komunity“* – většina sociálních sítí poskytuje prostor pro vytváření a účast ve „skupinách“. Tato funkce umožňuje uživatelům sdružovat se do komunit kolem sdílených zájmů a různých tématických okruhů.
- *„Obchodní funkce“* - dnešní sociální sítě rovněž poskytují různé obchodní funkce, které umožňují firmám a uživatelům prodávat nebo nakupovat produkty přímo na platformě.[23]

V dnešní době stále více jedinců z naší populace balancuje mezi reálným a virtuálním světem. Sociální sítě se téměř pro každého na této planetě staly neodmyslitelnou součástí jejich životů. Lze tedy říci, že tento stále se vyvíjející fenomén našeho digitálního věku zásadně mění způsob, jakým lidé komunikují, sdílejí informace a budují vztahy. Tato kapitola se dále zaměří na historii sociálních

[23] Přispěvatelé Wikipedie, Sociální síť [online], Wikipedie: Otevřená encyklopedie, c2024, Datum poslední revize 25. 02. 2024, 18:37 UTC, [citováno 29. 02. 2024]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Soci%C3%A1ln%C3%AD_s%C3%AD%C5%A5&oldid=23691281
CZ.NIC. Nebojte se internetu [online]. [cit. 2024-02-29]. Dostupné z: https://www.nebojteseinternetu.cz/page/3396/socialni-site/

sítí, jejich druhy, představení těch nejpopulárnějších a jejich dopad na mezilidské vztahy, komunikaci a kulturu.

1.3.1 Historie sociálních sítí

Samotné sociální sítě mají velmi hluboké kořeny v historii celé digitální komunikace a sociální interakce, neboť některé, z již zmíněných rysů byly jednotlivě představeny již v minulosti. Vývoj sociálních sítí je velmi zajímavým průvodcem evoluce tohoto odvětví internetového prostoru a rovněž způsobů, jakými lidé navzájem komunikují a sdílejí své životy v dnešní digitální době.

Počátky - Sociální sítě, jak je známe dnes, nemají dlouhou historii. Jejich kořeny sahají do 70. let 20. století, kdy se objevily první online platformy s prvky sociální interakce. Tyto platformy, jako například BBS (Bulletin Board Systems), umožňovaly uživatelům sdílet informace a komunikovat mezi sebou v online prostředí.

První "skutečná" sociální síť - První platformou, která je obecně považována za "skutečnou" sociální síť, je SixDegrees.com. Tato síť byla spuštěna v roce 1997 a umožňovala uživatelům vytvářet profily, navazovat kontakty s přáteli a známými a prohlížet profily druhých. SixDegrees.com zaznamenala značný úspěch a inspirovala vznik dalších podobných platforem.

Raný vývoj - V roce 2003 se objevily platformy LinkedIn a MySpace, které se zaměřily na specifické cílové skupiny. LinkedIn se zaměřil na profesní networking a budování kariéry, zatímco MySpace se stal populární platformou pro sdílení hudby a navazování kontaktů mezi mladými lidmi.

Facebook a další inovace - Rok 2004 znamenal zlom v historii sociálních sítí s uvedením platformy Facebook. Facebook, původně určený pouze pro studenty Harvardovy univerzity, se brzy rozrostl do globální sítě s miliardami uživatelů. Facebook přinesl inovace v podobě News Feedu, který uživatelům umožňuje sledovat aktivity a příspěvky jejich přátel.

Další inovace v oblasti sociálních sítí přinesly platformy jako YouTube (2005) a Twitter (2006). YouTube umožnil uživatelům sdílet videa a stal se tak dominantní

platformou pro online video obsah. Twitter se zaměřil na krátká textová sdělení (tweety) a stal se populárním nástrojem pro sdílení zpráv a informací v reálném čase.

Růst a diverzifikace - V posledních letech se objevilo mnoho dalších platforem s různou specializací. Instagram, založený v roce 2010 se zaměřuje na sdílení fotografií a videí a stal se populární mezi mladými uživateli. TikTok založený roku 2016 přinesl krátká videa s hudebním doprovodem a v krátké době dosáhl obrovské popularity a to zejména mezi mladšími uživateli.

Současný trend - Sociální sítě se stávají stále více integrovanými do běžného života. Lidé je používají pro komunikaci, sdílení informací, zábavu i marketingové účely. S rostoucím vlivem sociálních sítí se však také zvyšují obavy o ochranu osobních údajů a bezpečnost uživatelů.[24]

1.3.2 Druhy sociálních sítí

V této práci bych chtěl dále interpretovat druhy sociálních sítí. V rámci odborné literatury se setkáváme s různými děleními sociálních sítí. V následujících textech je uvedený podrobný přehled toho, jak lze veškeré sociální sítě dělit.

Profilově orientované sociální sítě: Jsou zaměřeny především pro vytváření uživatelských profilů. Patří mezi ně platformy jako Facebook nebo MySpace.

Obsahově zaměřené sociální sítě: Zde je klíčový především jejich obsah. Příkladem jsou služby jako YouTube pro sdílení videa nebo Flickr pro sdílení fotografií.

Sociální sítě "White-label": Umožňují uživatelům vytvořit vlastní sociální síť. Patří sem platformy jako PeopleAggregator a Ning.

---

[24] WIKISOFIA. Sociální síť [online]. [cit. 2024-02-29]. Dostupné z: https://wikisofia.cz/wiki/Sociální_síť
Přispěvatelé Wikipedie, Sociální síť [online], Wikipedie: Otevřená encyklopedie, c2024, Datum poslední revize 25. 02. 2024, 18:37 UTC, [citováno 29. 02. 2024]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Soci%C3%A1ln%C3%AD_s%C3%AD%C5%A5&oldid=23691281
MARYVILLE UNIVERSITY. The Evolution of Social Media: How Did It Begin, and Where Could It Go Next? [online]. [cit. 2024-02-29]. Dostupné z: https://online.maryville.edu/blog/evolution-social-media/

Virtuální sociální sítě: Nejsou sítě jako takové, ale nabízejí online virtuální prostředí. Převážně se jedná i videoherní prostředí. Mezi ně patří World of Warcraft, Minecraft, a další MMORPG (Massive Multiplayer Online Role Playing Game).

Micro-blogovací sociální sítě: Umožňují uživatelům zveřejňovat krátká sdělení přístupná ostatním uživatelům. Sem spadá zejména Twitter.[25]

1.3.3 Nejznámější sociální sítě v ČR

Pro lepší pochopení bezpečnostních rizik na sociálních sítí je třeba čtenáři představit, jaké sociální sítě, se kterými jsou tato rizika spojována, jsou v České republice nejvíce využívány a rovněž přiblížit jak tyto sociální sítě fungují.

Facebook – Všestranná sociální síť, která umožňuje uživatelům sdílet obsah, komunikovat a navazovat kontakty. Uživatelé mohou sdílet texty, obrázky, videa, odkazy a další obsah. Platforma také nabízí funkce pro vytváření skupin a stránek, propojení s přáteli a rodinou a sledování novinek a událostí. Facebook byl založen v roce 2004 Markem Zuckerbergem a původně byl určen pouze pro studenty Harvardovy univerzity. Platforma se však brzy rozrostla do globální sítě s miliardami uživatelů. V České republice byl Facebook spuštěn v roce 2008 a v současnosti má 5,5 milionu uživatelů v ČR.

YouTube - Platforma pro sdílení a sledování videí. Uživatelé mohou nahrávat, sledovat a komentovat videa. Platforma nabízí širokou škálu obsahu, včetně filmů, televizních pořadů, hudebních videí, tutoriálů a vlogů. YouTube byl založen v roce 2005 Chadem Hurleym, Stevem Chenem a Jawed Karim. V roce 2006 byl koupen společností Google a stal se dominantní platformou pro online video. V České republice byl YouTube spuštěn v roce 2008 a v současnosti má více než 8 milionu aktivních uživatelů v ČR.

Instagram - Platforma pro sdílení fotografií a krátkých videí. Uživatelé mohou přidávat filtry a efekty ke svým fotografiím a sdílet je s přáteli a sledujícími.

[25] INTERNETEM BEZPEČNĚ. Sociální sítě [online]. [cit. 2024-02-29]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/socialni-media/socialni-site/

Platforma také nabízí funkce pro sdílení živého videa a zpráv. Instagram byl založen v roce 2010 Kevinem Systromem a Mikem Kriegerem. V roce 2012 byl koupen společností Facebook a stal se populární platformou pro sdílení osobních a kreativních fotografií a videí. V České republice byl Instagram spuštěn v roce 2012 a v současnosti zde má 2,5 milionu uživatelů.

Twitter (v současné době přejmenován na X) - Platforma pro sdílení krátkých textových zpráv, tzv. tweetů. Tweety mohou obsahovat text, obrázky, videa a odkazy. Uživatelé mohou sledovat jiné uživatele a retweetovat jejich tweety. Twitter byl založen v roce 2006 Jackem Dorseym, Noahem Glassem, Biz Stoneem a Evanem Williamsem. Tato sociální síť se stala populární platformou pro sdílení rychlých zpráv, komentování aktuálních událostí a komunikaci s influencery. V České republice byl Twitter spuštěn v roce 2008 a v současnosti zde má více než 600 000 uživatelů.

TikTok – Sociální síť určena pro sdílení krátkých videí, tzv. TikToků. Uživatelé mohou nahrávat videa s hudbou, efekty a filtry a sdílet je s přáteli a sledujícími. Platforma je oblíbená mezi mladší generací a stala se důležitým nástrojem pro marketing a influencer marketing. TikTok byl spuštěn v roce 2016 a v současnosti má přes 1 miliardu aktivních uživatelů ve více než 150 zemích světa. Tato sociální síť má v budoucnu velký potenciál v počtu uživatelů v ČR předehnat i Facebook nebo Instagram.

Snapchat - Platforma pro sdílení fotografií a videí, které se po krátké době automaticky smažou. Uživatelé mohou přidávat text, filtry a efekty ke svým fotografiím a videím a sdílet je s přáteli a sledujícími. Platforma je oblíbená mezi mladší generací a stala se důležitým nástrojem pro zábavu a komunikaci. Snapchat byl spuštěn v roce 2011 a v současnosti má přes 330 milionů aktivních uživatelů ve více než 200 zemích světa. V České republice má Snapchat 1 000 000 aktivních uživatelů.[26]

[26] KRYTOLAND. Nejpoužívanější sociální sítě v České republice [online]. [cit. 2024-02-29]. Dostupné z: https://www.krytoland.cz/clanek-nejpouzivanejsi-socialni-site-v-ceske-republice

2 Bezpečnost a možná rizika na sociálních sítích

V této kapitole bude objasněna problematika týkající se bezpečnosti a možných rizik na sociálních sítí, přičemž budou čtenáři popsány jednotlivá rizika, která se v souvislosti s používáním sociálních sítí objevují a jsou nejčastější.

Bezpečnost na sociálních sítích

Bezpečnost na sociálních sítích je klíčovým aspektem digitálního světa, kterému by měla být věnována značná pozornost všech uživatelů. Uživatelé sociálních sítí by měli být obezřetní zejména při sdílení osobních informací a měli by si pečlivě nastavit „svá soukromí“ aby minimalizovali riziko zneužití dat a kyberšikany (dnešní sociální sítě umožňují uživatelům spravovat soukromí svých účtů a tím omezovat přístup k datům, které uživatelé sdílejí).

Možná rizika na sociálních sítích

V souvislosti s používáním sociálních sítí existuje mnoho rizik. Pro účely této práce byly vybrány zejména následující:

- *Kyberšikana*: Jedním z nejvážnějších problémů spojených s užíváním sociálních sítí je kyberšikana. Kyberšikana se stává stále závažnějším problémem, zejména mezi mladými lidmi. Může mít vážné psychologické důsledky a vést k emocionálnímu traumatu a snížení sebeúcty. [27]
- *Zneužití osobních údajů*: Sociální sítě často shromažďují rozsáhlé množství osobních údajů o svých uživatelích, což může být zneužito ke sledování a identifikaci osob. Zneužití osobních údajů je jedním z hlavních faktorů, které mohou zvyšovat zranitelnost uživatelů při používání sociálních sítí. [28]
- *Dezinformace, Fake news a hoaxy*: Sociální sítě jsou často prostředím pro šíření dezinformací a falešných zpráv, což může mít škodlivé důsledky pro společnost a jednotlivce. Při zkoumání vlivu sociálních médií na společnost

[27] ŠMAHAJ, Jan. Kyberšikana jako společenský problém: Cyberbullying as a social problem. Olomouc: Univerzita Palackého v Olomouci, 2014. ISBN 9788024442273.
[28] KOLOUCH, Jan. CyberCrime. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7.

je třeba zdůraznit, že šíření dezinformací je dalším z nejzávažnějších problémů, kterým musíme čelit v digitálním věku.[29]

- *Online predátoři*: Na sociálních sítích mohou operovat online predátoři, kteří se snaží získat důvěru a kontakt s nezletilými uživateli za účelem sexuálního vykořisťování nebo získání osobních informací.[30]
- *Závislost na sociálních médiích*: Užívání sociálních sítí může vést k vytváření závislosti a negativně ovlivnit duševní zdraví jednotlivců. Nadměrné používání sociálních médií může vést k úzkosti, depresi nebo pocitu izolace.[31]

2.1 Kyberšikana

Jedním z nejzásadnějších bezpečnostních rizik na sociálních sítích je bezesporu kyberšikana. V odborné literatuře je kyberšikana definována různě, avšak téměř vždy má definice totožný význam. Pro tuto práci byla vybrána definice z knihy Bezpečně n@ internetu od Martina Kožíška a Václava Píseckého, ve které tito autoři uvádí, že: „*Kyberšikana je jakékoliv chování, jehož záměrem je vyvést z rovnováhy, ublížit, zastrašit nebo jinak ohrozit oběť za pomoci moderních informačních technologií.*“[32]

2.1.1 Prostředky k realizaci kyberšikany

Existuje celá řada prostředků v online prostoru, které mohou být využity pro kyberšikanu. Podle publikace s názvem Kyberšikana. Průvodce novým fenoménem od Aleny černé a kol. mezi hlavní prostředky k realizaci kyberšikany patří tyto:

- Sociální sítě: Kyberšikana na sociálních sítích často zahrnuje urážlivé komentáře a sdílení nevhodných obsahů.

[29] KIRKPATRICK, David. Pod vlivem Facebooku: příběh z nitra společnosti, která spojuje svět. Brno: Computer Press, 2011. ISBN 9788025135730.
[30] ECKERTOVÁ, Lenka a DOČEKAL, Daniel. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. Brno: Computer Press, 2013. ISBN 9788025138045.
[31] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016. ISBN 9788024755953.
[32] 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

- Online interaktivní hry: Kyberšikana v online hrách může zahrnovat napadání, vyloučení ze skupin a organizované útoky na hráče.
- Webové stránky: K ublížení oběti může sloužit i již existující webové platformy, jako je YouTube, kam kdokoli může nahrát video. Pod videa lze zveřejňovat urážlivé komentáře.
- Instant messaging (IM) a zprávy (SMS a MMS): Instant messaging aplikace jako Messenger nebo Instagram DMs mohou být také využity ke kyberšikaně prostřednictvím urážlivých zpráv. Stejně mohou být využity i SMS a MMS zprávy.
- Blogy: Pomocí blogu lze šířit různé nevhodné materiály týkající se oběti.
- Elektronická pošta (e-mail): E-mailové zprávy mohou být také zneužity k posílání urážlivých či nevhodných obsahů.
- Chatovací místnosti: Tyto webové stránky slouží k seznamování a komunikaci. Agresor se zde může vydávat za kohokoliv, zjišťovat intimní informace a později je zneužít.
- Internetové ankety a dotazníky: Tyto formy mohou být využity k sestavování dotazníků, které zahrnují nepříjemné otázky nebo hodnocení.[33]

2.1.2 Formy kyberšikany

Kyberšikana se může projevovat různými způsoby, přičemž Alena Černá a kol. ve své knize s názvem Kyberšikana. Průvodce novým fenoménem je ve své publikaci uvádí následovně:

- *Vyloučení a ostrakizace*: Tento projev kyberšikany spočívá v tom, že oběť je záměrně vyloučena ze skupiny, online komunity nebo sociálního kruhu. To může vést k pocitu izolace, osamělosti a nedostatečného začlenění, což může negativně ovlivnit duševní zdraví oběti.
- *Vydávání se za někoho jiného a krádež hesla*: Tento druh kyberšikany spočívá v tom, že agresor přebírá identitu oběti a vytváří falešné profily nebo účty na sociálních sítích či jiných online platformách. Agresoři mohou

[33] ČERNÁ, Alena. Kyberšikana: průvodce novým fenoménem. Psyché (Grada). Praha: Grada, 2013. ISBN 9788024745770.

také krást hesla k účtům oběti a zneužívat je k šíření nepřátelských komentářů nebo škodlivých informací.

- *Kyberharašení a kyberstalking*: Kyberharašení je forma kyberšikany, při které agresor opakovaně obtěžuje oběť prostřednictvím svého agresivního chování v online prostoru, zasíláním nevyžádaných zpráv nebo výhrůžek. Kyberstalkingu zahrnuje zejména sledováním oběti, vytváření falešných profilů či šířením osobních (intimních) informací o oběti s cílem ji zastrašit nebo utlačovat.
- *Flaming*: Flaming je termín označující ostrý verbální konflikt mezi jednotlivci na internetových fórech, diskusních skupinách nebo chatovacích místnostech. Tento druh kyberšikany je charakterizován agresivním a urážlivým jazykem, který má za cíl zesměšňovat, napadat nebo ponižovat svou oběť.
- *Pomlouvání*: Pomlouvání v kyberprostoru spočívá v šíření nepravdivých nebo zavádějících informací o oběti s cílem poškodit její pověst, reputaci nebo sociální postavení. Tato forma kyberšikany může mít vážné důsledky pro oběť, včetně emočního stresu a sociálního vyloučení.
- *Odhalení a podvádění*: Tento projev kyberšikany zahrnuje sdílení osobních informací o oběti, jako jsou fotografie, videa nebo soukromá korespondence, bez jejího souhlasu. Tím dochází k porušení soukromí a možnému poškození oběti, která se může cítit vystavena veřejnému ponížení nebo šikaně.
- *Happy slapping*: Happy slapping je forma kombinující fyzické a kybernetické napadení, kdy je oběť fyzicky napadena a útok je zaznamenán videokamerou nebo mobilním telefonem a následně sdílen v online prostoru. Tento projev kyberšikany může mít vážné fyzické i emoční následky pro oběť.[34]

[34] ČERNÁ, Alena. Kyberšikana: průvodce novým fenoménem. Psyché (Grada). Praha: Grada, 2013. ISBN 9788024745770.

2.2 Zneužití osobních údajů

V souvislosti s užíváním sociálních sítí často uživatelé zpřístupňují své osobní údaje, které mohou být zneužity případně využity k páchání trestné činnosti či jiným útokům v kyberprostoru.

Dle definice § 4 písm. a) z již zrušeného zákona č.101/2000 Sb., o ochraně osobních údajů, je osobní údaj: „*Jakákoliv informace týkající se určené nebo určitelné fyzické osoby, k níž se osobní údaje vztahují. Tato se považuje za určenou nebo určitelnou, jestliže lze fyzickou osobu přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro její fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu*“.[35]

Některé osobní údaje jsou považovány za citlivé, protože mohou odhalit informace o zdravotním stavu, sexuálních preferencích, náboženských a politických přesvědčeních nebo osobních názorech konkrétní osoby.

K vylákání osobních údajů používají útočníci nejčastěji tyto techniky:

Phishing - Tato technika spočívá v tom, že se útočníci vydávají za důvěryhodné osoby, organizace nebo weby, aby získali citlivé údaje jako hesla, bankovní účty nebo platební karty. Útoky phishingem často probíhají pomocí e-mailů nebo sociálních sítí s falešnými informacemi, které vypadají jako legitimní. Tyto zprávy mohou obsahovat odkazy na padělané weby, které napodobují skutečné bankovní portály nebo korporátní systémy. Falešné e-maily a zprávy často vzbuzují naléhavost nebo strach, což vede k rychlé reakci oběti. Když oběť poskytne své údaje na padělaném webu, jsou okamžitě odeslány útočníkovi.

Sociální inženýrství – Podvodný trik, který používají podvodníci k tomu, aby vás přiměli k odhalení citlivých informací nebo k provedení určitých akcí, které jsou v jejich prospěch. Je to druh podvodu, který využívá lidský faktor, který bývá nejčastěji tím nejslabším článkem v celém bezpečnostním systému.

[35] Viz § 4 Zákona č. 101/2000 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) v posledním znění

Tento trik má svůj vlastní postup k získání potřebných citlivých údajů:

Výzkum: Útočník sbírá informace o vás, jako jsou vaše jméno, pracovní pozice, informace na sociálních sítích a další osobní údaje, aby získal vaši důvěru.

Přesvědčivý příběh: Na základě těchto informací vytvoří *přesvědčivý příběh*, pomocí kterého vás zmanipuluje.

Manipulace: Útočník může předstírat, že je zaměstnancem nebo obchodním partnerem a žádat o důvěrné informace. Často to dělají pomocí telefonních hovorů.

Tlak na akci: Často vás tlačí k rychlému jednání, vytvářejí iluzi naléhavosti nebo vyhrožují negativními důsledky v případě nekonání.

Získání informací: Pokud se jim to podaří, získají od vás citlivé informace nebo vás přimějí k akcím, jako je otevření virem napadených e-mailových příloh nebo poskytnutí přístupových kódů.

Zneužití informací: Nakonec zneužijí vaše informace k nelegálním aktivitám, kterými jsou nejčastěji krádež identity nebo neoprávněné transakce.

Vishing - Vishing je jakousi obdobou phishingu, ale namísto e-mailů nebo textových zpráv používá hlasovou komunikaci, jako jsou telefonní hovory nebo hlasové zprávy, aby vás přesvědčili k poskytnutí osobních nebo bankovních údajů. Podvodníci často využívají zastrašování nebo naléhavost situace, aby vás přiměli k okamžité reakci. Tvrdí například, že byla zaznamenána podezřelá aktivita na vašem bankovním účtu nebo že váš účet bude zrušen, pokud neposkytnete požadované informace.

Smishing - Podvodná aktivita podobná phishingu a vishingu, ale namísto e-mailů nebo telefonních hovorů se útočníci snaží klamat prostřednictvím SMS nebo obdobných zpráv. Útočníci posílají textové zprávy, které vypadají jako zprávy od legitimních organizací, jako jsou banky, přepravní společnosti nebo státní instituce. Často lákají oběti k akci, která vyžaduje poskytnutí osobních nebo finančních informací. Textová zpráva může obsahovat naléhavé výzvy k akci, například varování o podezřelé aktivitě na účtu nebo lákavé nabídky. Tyto zprávy často obsahují odkazy na falešné webové stránky, které vypadají jako oficiální

stránky a žádají vás o zadání citlivých údajů, čísla bankovního účtů nebo čísla platební karty.

Spoofing - Způsob podvodu, při kterém se útočník vydává za jinou osobu, zařízení nebo uživatele, aby získal neoprávněný přístup k datům, šířil malware, oklamal oběti nebo získal citlivé informace a obešel bezpečnostní opatření zejména pomocí:
Falešných e-mailů, přičemž útočník odesílá e-maily s podvrženou hlavičkou, aby vypadaly jako z důvěryhodného zdroje, jako je banka nebo známý jedinec. Tento trik je často používán při phishingových útocích.

Falešných telefonních čísel nebo SMS, kdy útočník mění informace na volajícím ID, aby se zdálo, že hovor pochází z legitimního zdroje, jako jsou úřady, policie nebo banky. Může například volat z cizí země s pomocí služby změny ID volajícího (některé země tuto službu nabízí).

Podvržených webových stránky v rámci čehož útočník vytváří falešné verze důvěryhodných webových stránek, aby vás přesvědčil k zadání svých osobních údajů nebo přihlašovacích údajů.[36]

2.3 Dezinformace, fake news a hoaxy

Pomocí sociálních sítí jsou rovněž šířeny dezinformace, fake news a hoaxy. Bezpečnostním rizikem na sociálních sítích jsou zejména proto, že se skrze sociální sítě velmi rychle šíří a velká část populace těmto nepravdivým a zkresleným informacím podléhá a jsou tak přesvědčeni o jejich pravdivosti.

Dezinformace - Úmyslně vytvořené nepravdivé informace, které mají záměrně ovlivnit naše myšlení. Jejich šíření může negativně ovlivnit celou společnost. Cílem dezinformací je přesvědčit nás, že jsou pravdivé, i když ve skutečnosti nejsou. Často bývají součástí zahraniční propagandy jako součást strategie hybridní války nebo též součástí politické kampaně.

[36] MĚŠEC.CZ. Vyznejte se v podvodech. Co je phishing, vishing, smishing a spoofing? [online]. [cit. 2024-02-29]. Dostupné z: https://www.mesec.cz/clanky/vyznejte-se-v-podvodech-co-je-phishing-vishing-smishing-ransomware-a-dalsi/

Fake news - Termín "fake news" je termín, který označuje nepravdivé zprávy, ale taktéž samotná média, která je šíří. V českém prostředí se častěji používají pojmy "dezinformační weby" nebo "dezinformační média", ale mohou sem patřit i bulvární média, která šíří nepravdivé informace. Důležité je uvědomit si, že mezi fake news určitě nepatří satirická ani humoristická média.

Hoax - Typ falešné zprávy, která se snaží vyvolat paniku nebo strach a přimět lidi k rychlým a nerozvážným reakcím. K hoaxům patří zprávy s humorem nebo satirou, které mají za cíl pobavit čtenáře. Rovněž sem spadají falešné petice, prosby o pomoc, řetězové dopisy nebo různé městské legendy. Skutečným bezpečnostním rizikem jsou však zprávy, které šíří informace o nebezpečí, které neexistuje, uvádějí zkreslené informace o aktuálních problémech, poskytují nebezpečné rady nebo jsou součástí online podvodů.[37]

2.4 Online predátoři

K rozmachu sociálních sítí bezesporu patří seznamování se skrze online prostředí. Při tomto druhu seznamování je však nutné být velmi obezřetný, neboť mezi novými kontakty můžeme narazit i na tzv. „online predátory“. V souvislosti s online predátory je třeba zdůraznit, že jsou to lidé, kteří skrze kyberprostor navazují kontakty s lidmi, a to především s dětmi (jsou zaznamenány i případy týkající se dospělých osob), přičemž následně svou oběť obtěžují nebo zneužívají. Podle doc. Mgr. Kamila Kopeckého, Ph.D. se dají podle závažnosti své činnosti rozdělit do těchto kategorií:

“*Honiči/Masturbátoři*” – Pro tuto kategorii predátorů je kontakt s obětí pouze cestou k „osobnímu uspokojení“. Tito predátoři od svých obětí nevyžadují žádné intimní materiály, nevydírají je, nechtějí se s nimi scházet mimo kyberprostor. Jde jim pouze o uspokojení před člověkem, kterého zdánlivě znají.

“*Zoufalci*” – Tito predátoři mají problémy s navázáním kontaktu s dospělými osobami a zpravidla se tedy uchylují k seznámení se v kyberprostoru s dětmi,

[37] E - BEZPEČÍ. Co je to vlastně ten hoax, dezinformace, misinformace nebo třeba fake news? Čím se tyto termíny liší a co mají společného? [online]. [cit. 2024-02-29]. Dostupné z: https://www.e-bezpeci.cz/index.php/clanky-komentare/2864-co-je-to-vlastne-ten-hoax-dezinformace-misinformace-nebo-treba-fake-news-cim-se-tyto-terminy-lisi-a-co-maji-spolecneho

neboť je to pro ně snazší díky tomu, že jsou snadno ovlivnitelné. Tento druh predátorů také od svých obětí nevyžaduje žádné intimní materiály, nechtějí se s nimi scházet mimo kyberprostor a nevydírají je, nicméně mohou trpět některou formou parafilie.

Predátor úroveň I - Abuzér – Tento predátor již svou oběť obtěžuje s cílem ji zneužít. Zpravidla svou oběť tlačí k poskytnutí intimních materiálů nebo ji pobízí ke vzájemným sexuálním aktivitám v rámci kyberprostoru, čehož zneužívá k výrobě pornografického materiálu, nicméně se jeho jednání stále vztahuje pouze ke kyberprostoru a svou oběť nenutí k osobním schůzkám.

Predátor úroveň II - Vyděrač – Do této kategorie predátorů spadají ti, kteří splňují podmínky „Abuzéra“, ale zároveň své oběti vyhrožují zveřejněním získaných intimních materiálů v online prostředí (mezi jeho známými), pokud od nich neobdrží peníze či jiné benefity, popř služby či další intimní materiál. Zveřejněním vyhrožují rovněž v případě, že oběť někomu o predátorovi řekne. Tento predátor také svou oběť nenutí k osobnímu setkání.

Predátor úroveň III - Kybergroomer -Tento typ predátora je tím nejvíce nebezpečným, neboť kombinuje predátora úrovně I a II, přičemž se snaží vynutit si osobní kontakt s obětí v reálném světě mimo kyberprostor. Na těchto schůzkách pak často dochází k pohlavnímu zneužití, znásilnění a další závažné trestné činnosti.[38]

2.4.1 Kybergrooming

Kybergrooming představuje zřejmě nejzávažnější hrozbu v online prostředí. Jedná se o rizikovou formu komunikace mezi dospělou osobou a dítětem, která cílí na zneužívání dítěte. Cílem kybergroomingu je vybudovat si důvěru s vybranou dětskou obětí a následně ji nalákat na osobní setkání v reálném světě.

[38] DOC. MGR. KOPECKÝ KAMIL PH.D. E - BEZPEČÍ. Rodiče, nepanikařte! Film V síti je sice syrový, ale bezpečnost dětí v online prostředí není těžké zabezpečit. Stačí se držet několika rad! [online]. [cit. 2024-02-29]. Dostupné z: https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1791-rodice-nepanikarte-film-v-siti-je-sice-syrovy-ale-bezpecnost-deti-v-online-prostredi-neni-tezke-zabezpecit-staci-se-drzet-nekolika-rad

Zde se pak „otevírají dveře“ k závažným formám zneužití, ať už se jedná o sexuální napadení, produkci dětské pornografie, prostituci, fyzické násilí, či zneužívání pro jiné nekalé účely, jako je terorismus.

Kybergrooming se vyznačuje rafinovanými metodami manipulace, které predátor používá k získání kontroly nad dítětem a následným domluvením si schůzky, kde dochází k pokračující manipulaci (přemlouvání, nabídky, focení) a případně k útoku (sexuálnímu, fyzickému). Mezi tyto metody patří zejména:

Zrcadlení - Predátor se snaží napodobovat chování a zájmy oběti, aby si s ní vybudoval důvěryhodný vztah.

Phishing - Snaha o získání osobních informací o dítěti a jeho rodině a následné profilování oběti, kdy predátor analyzuje její slabé stránky, aby věděl, jak ji nejlépe zmanipulovat.

Vábení (luring) a uplácení - Predátor se snaží snižovat zábrany dítěte zaváděním sexuálních témat do konverzace a postupně ho tak otevírá svému vlivu. Rovněž se snaží dítě uplatit různými dary nebo přímo finanční hotovostí.

Izolační metody -Slouží k oddělení oběti od jejích blízkých a posílení kontroly predátora.

Manipulace pomocí fotografií – Jedná se o vylákání fotografií pomocí zasílání intimních fotografií opačného pohlaví a vydávání se za osoby zachycené na zaslané fotografii.

Webcam trolling – Vyznačuje se zejména snahou o svlékání či sexuální aktivity před webkamerou a řadí se tak mezi další znepokojivé nástroje predátorů.[39]

2.5 Závislost na sociálních mediích

Problém závislosti na sociálních sítích nastává, když jednotlivec investuje nadměrný čas a pozornost do užívání těchto digitálních platforem a má potíže s jejich omezením či opuštěním. Tato závislost může vyvolat řadu negativních dopadů na jak fyzické, tak duševní zdraví jedince, a to jak krátkodobě, tak i dlouhodobě.

[39] KYBERGROOMING. KYBERGROOMING rizikové seznamování v online prostředí [online]. [cit. 2024-02-29]. Dostupné z: https://www.kybergrooming.cz

Příčiny vzniku závislosti

Dopaminová odměna: Sociální média stimulují uvolňování dopaminu v mozku, neurotransmiteru hrajícího klíčovou roli v systému odměn. To vede k pocitu uspokojení a posiluje chování, které k jeho uvolnění vedlo, v tomto případě opakované používání sociálních sítí.

Sociální izolace: Sociální média slouží jako alternativa k reálné sociální interakci a pro osoby trpící osamělostí či sociální izolací představují možnost spojení s druhými. Pocit sounáležitosti a sdílení s komunitou na sociálních sítích tak může zmírnit negativní dopady izolace.

FOMO (Fear of Missing Out): Strach z promeškání důležitých událostí nebo zážitků, které sdílí online přátelé, je silným motivátorem k neustálému sledování sociálních sítí. Uživatelé se tak snaží minimalizovat riziko, že jim něco unikne, a udržují si pocit informovanosti a propojení s online světem.

Stres a únik od reality: Internet a sociální média slouží jako útočiště před stresem a problémy reálného světa. Poskytují tak rozptýlení a možnost uniknout do virtuálního světa, kde se uživatelé mohou cítit uvolněněji a bezstarostněji.

Dopady závislosti

Psychické zdraví:

Úzkost a deprese: Neustálý příval informací a sociální srovnávání na platformách může vést k chronickému stresu, úzkosti a depresivním symptomům.

Snížené sebevědomí: Negativní komentáře, nereálné standardy krásy a idealizované životy prezentované online můžou vést k pochybnostem o sobě a nízkému sebevědomí.

Pocit osamělosti: Paradoxně i přes propojení s online komunitou se u závislých uživatelů může prohlubovat pocit izolace a osamělosti v reálném světě.

Nerovnoměrné zatížení mozku: Přemíra stimulace a multitasking při používání sociálních sítí brání mozku v adekvátní regeneraci a vede k jeho únavě a vyčerpání.

Fyzické zdraví:

Obezita a sedavý způsob života: Dlouhé hodiny strávené vsedě před obrazovkou bez dostatku fyzické aktivity přispívají k nárůstu váhy a riziku obezity.

Spánkové poruchy: Modré světlo z obrazovek narušuje produkci melatoninu, hormonu spánku, a vede k problémům s usínáním a nekvalitnímu spánku.

Bolesti zad a krční páteře: Nevhodná ergonomie a nesprávné držení těla při používání mobilních zařízení můžou vést k bolestem zad a krční páteře.

Zhoršování zraku: Nadměrné namáhání očí při sledování obrazovek zblízka může vést k únavě očí a v dlouhodobém horizontu k trvalému zhoršení zraku.

Sociální vztahy:

Narušené vztahy: Závislost na sociálních sítích může vést k zanedbávání osobních a pracovních povinností, čímž se narušují vztahy s partnerem, rodinou a přáteli.

Komunikační problémy: Nadměrná online komunikace může vést k zhoršení komunikačních dovedností a neschopnosti efektivně komunikovat v reálném světě.

Omezení sociálních interakcí: Uživatelé závislí na sociálních sítích se můžou vyhýbat reálným sociálním interakcím a preferovat online komunikaci, čímž se omezuje jejich sociální život.[40]

[40] FINEFIFTY. Závislost na internetu a sociálních sítích: velké nebezpečí moderního světa [online]. [cit. 2024-02-29]. Dostupné z: https://fine50.cz/zavislost-na-internetu-a-socialnich-sitich-velke-nebezpeci-moderniho-sveta/

3 Nejzranitelnější skupiny uživatelů a prevence jednotlivých bezpečnostních rizik

Bezpečnostní rizika vznikající v souvislosti s používáním sociálních sítí jsou úzce spjata převážně s dětmi, teenagery a mladými dospělými (6 – 30 let), kteří sociální sítě využívají nejvíce.

Prevence bezpečnostních rizik vznikajících v souvislosti s užíváním sociálních sítí by se dala rozdělit do několika skupin, podle toho, kdo ji může realizovat:

1. **Rodiče** hrají klíčovou roli v ochraně dětí před riziky virtuálního světa. Otevřená komunikace s dětmi ze strany jejich rodičů o online rizicích je zcela zásadní, přičemž je důležité zdůraznit, že ne vše, na co děti ve virtuálním světě narazí je pravdivé, a že se lidé nemusí chovat tak, jak se prezentují online. Vzájemná komunikace a důvěra by měla vést ke sdílení online zážitků mezi dětmi a rodiči, což je klíčové pro správnou prevenci v této oblasti. Rodiče by rovněž neměli zanedbávat případné změny chování spojené s dětskými návštěvami v online prostředí, neboť tyto mohou poukazovat na vzniklé potíže.
2. **Škola** hraje další podstatnou roli v prevenci online rizik u dětí, které nemají oporu v rodině, ale též může působit podpůrně společně s rodiči. Pokud se dítě necítí komfortně svěřovat se rodičům, škola by mu měla poskytnout prostor a podporu pro sdílení problémů týkajících se jak toho reálného světa, tak toho virtuálního.
3. **Neziskové organizace, televizní pořady a stanice, preventivní projekty, státní složky a orgány.** Tito všichni a spousta dalších se svou aktivní účastí podílí na prevenci týkající se virtuálního prostředí, a to různými přednáškami ve školách, prezentacemi, reportážemi, články, aktivní pomocí při vzniklých problémech a dalšími aktivitami. Jedná se především o Policii ČR, Dětské krizové centrum, projekt E-bezpečí, Bílý kruh bezpečí, linka bezpečí.

I přes obecné informace ke zranitelným skupinám a prevenci, týkající se této problematiky, zde existují určitá specifika u každé jednotlivé hrozby (tyto hrozby již byly představeny v předchozí kapitole.)[41]

Kyberšikana

Nejzranitelnější skupinu vůči kyberšikaně tvoří děti a teenageři. Zvýšené riziko se týká zejména těch, kteří disponují některou z níže uvedených charakteristik:

- *Plachost a stydlivost*: Tyto rysy omezují sociální interakce a ztěžují obranu proti kyberšikaně. Oběti se tak mohou cítit osamělé a bezmocné.
- *Nejistota*: Nižší sebevědomí a nízké sebehodnocení ztěžují zvládání psychického dopadu kyberšikany. Oběti se tak mohou stávat ještě více uzavřené a izolované.
- *Odlišnosti v barvě vlasů, pleti nebo stylu oblékání*: Tyto odlišnosti, které se odchylují od normy v daném kolektivu, se stávají záminkou pro posměšky a urážky rovněž v online prostředí.[42]

Zdeněk Martínek ve své knize Agresivita a kriminalita školní mládeže uvádí jakási pravidla **prevence**, kterými se řídit 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]

[41] KAVALÍR, Aleš (ed.). Kyberšikana a její prevence: příručka pro učitele. Plzeň: Pro město Plzeň zpracovala společnost Člověk v tísni, pobočka Plzeň, 2009. ISBN 9788086961781.
KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016. ISBN 9788024755953.
[42] Přispěvatelé Wikipedie, Kyberšikana [online], Wikipedie: Otevřená encyklopedie, c2024, Datum poslední revize 29. 01. 2024, 11:45 UTC, [citováno 29. 02. 2024]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Kyber%C5%A1ikana&oldid=23604206
[43] MARTÍNEK, Zdeněk. Agresivita a kriminalita školní mládeže. 2., aktualizované a rozšířené vydání. Praha: Grada, 2015. Pedagogika (Grada). ISBN 978-80-247-5309-6.

Zneužití osobních údajů

U zneužití osobních údajů nelze jednoznačně říci, která skupina je nejvíce ohrožená, nicméně u této hrozby je svým způsobem zranitelná každá věková skupina, a to díky svým různým vlastnostem.

Děti a teenageři: Nemají plně vyvinutý smysl pro kritické myšlení a mohou být snáze manipulovatelní. Často využívají sociální sítě a sdílí osobní informace online bez ohledu na rizika. Nemusejí si být vědomi důležitosti ochrany osobních údajů.

Senioři: Mohou být méně obeznámeni s online technologiemi a hrozbami. Mohou být náchylnější k podvodům a manipulaci. Mohou mít zhoršené kognitivní funkce, které jim ztěžují ochranu osobních údajů.

Lidé s vysokými příjmy: Mohou nakupovat na více online místech a tím zanechávat spousty dohledatelných digitálních stop

Prevence: Používání silných a jedinečných hesel pro každý účet a jejich pravidelná obměna. Zapnutí dvoufaktorového ověřování tam, kde je to možné, aby se při přihlašování vyžadovalo více než jen heslo. Obezřetnost při sdílení osobních údajů online a vyhýbání se sdílení citlivých informací na veřejných platformách. Udržování softwaru a antivirových programů aktualizované, aby se minimalizovala zranitelnost systému. Obezřetnost při otevírání odkazů v e-mailech nebo na webových stránkách a ověřování zdrojů. Sebevzdělávání a vzdělávání svých blízkých o možných rizicích.[44]

Dezinformace, fake news, hoaxy

Neexistuje jednoznačná odpověď na otázku, která věková skupina je nejvíce ohrožena dezinformacemi, hoaxy a fake news. Riziko se liší v závislosti na různých faktorech, kterým jsou zejména úroveň mediální gramotnosti, způsob konzumace informací, politické a ideologické postoje.

[44] LIFELOCK BY NORTON. Who Are the Biggest Targets for Identity Theft? [online]. [cit. 2024-02-29]. Dostupné z: https://lifelock.norton.com/learn/identity-theft-resources/identity-theft-targets

Nicméně, i zde jsou některé skupiny obecně považovány za více zranitelné:

Senioři: Mohou mít méně zkušeností s online technologiemi, a proto hůře rozlišují mezi pravdivými a nepravdivými informacemi. Mohou být více důvěřiví a náchylnější k manipulaci. Zpravidla mají menší síť kontaktů, která by jim pomohla ověřit informace.

Děti a teenageři: Nemusejí mít plně vyvinutý smysl pro kritické myšlení, a proto hůře hodnotí informace. Mohou být náchylnější k tlaku ze strany vrstevníků a sdílet dezinformace bez ověření. Často tráví více času online a mohou tak být více vystaveni dezinformacím.

Lidé s nízkými příjmy: Mohou mít omezený přístup k informacím a technologiím pro ověřování informací díky svému nízkému příjmu.

Prevence: Využití kritického myšlení a slepě všemu nevěřit. Ověřování si informací z více důvěryhodných zdrojů. Rozlišovat fakta a názory. Zvýšená opatrnost při sdílení informací na sociálních sítích. Nešířit informace, o jejichž pravdivosti nejsme přesvědčeni. Zdroje informací si lze rovněž ověřit na webových stránkách Ministerstva vnitra ČR v „seznamu dezinformačních internetových stránek v EU“.[45]

Online predátoři

Touto hrozbou virtuálního světa jsou nejvíce ohroženy děti a teenageři, protože mohou být snáze manipulovatelní, a proto často bývají skrze virtuální svět terčem osob s různými formami pedofílie. Mezi dětmi a teenagery jsou nejvíce zranitelné dívky a mladé ženy, které bývají nejčastěji terčem sexuálního obtěžování. Obecně lze říci, že obětmi bývají převážně lidé s nízkým sebevědomím, kteří se cítí osamělí nebo izolovaní v reálném světě a hledají tak „své místo“ ve světě virtuálním.[46]

[45] Příručka RESIST. In: Centrum proti hybridním hrozbám Ministerstva vnitra České republiky [online]. Praha: Ministerstvo vnitra České republiky, c2024 [cit. 2024-02-29]. Dostupné z: https://www.mvcr.cz/chh/soubor/resist-cz-pdf.aspx

[46] DOC. MGR. KOPECKÝ KAMIL PH.D. E - BEZPEČÍ. Rodiče, nepanikařte! Film V síti je sice syrový, ale bezpečnost dětí v online prostředí není těžké zabezpečit. Stačí se držet několika rad! [online]. [cit. 2024-02-29]. Dostupné z: https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1791-rodice-nepanikarte-film-v-siti-je-sice-syrovy-ale-bezpecnost-deti-v-online-prostredi-neni-tezke-zabezpecit-staci-se-drzet-nekolika-rad

Prevence: Nikdy nesdílet osobní informace s neznámými osobami online. Opatrnost při navazování online kontaktů. Nevěřit všemu, co o sobě neznámá osoba říká. Při pocitu ohrožení se vše sdělit důvěryhodné dospělé osobě, blízké osobě nebo přímo policii. Mluvit s dětmi o rizicích online predátorů. Sledování aktivit a komunikací dětí. Nastavení rodičovské kontroly na počítačích a mobilních zařízení.[47]

Závislost na sociálních médiích

Teenageři a mladí dospělí jsou obecně považováni za nejvíce ohroženou skupině, co se týče závislosti na sociálních médiích. Náchylní k této závislosti bývají zpravidla jedinci s nízkým sebevědomím, kteří trpí úzkostmi nebo depresemi, a kteří se cítí být osamělí nebo izolovaní v reálném světě. Tito lidé pak mohou na sociálních sítích hledat útěchu a útěk od reálného světa do toho virtuálního.

Prevence**:** Stanovení limitů pro používání sociálních sítí (určení, kolik času denně trávit na sociálních sítích). Vypínat si notifikace ze sociálních sítí, čímž se omezí nutkání neustále kontrolovat telefon. Vyhledávání jiných aktivit - sport, koníčky, trávení času s přáteli a rodinou (v reálném světě). Aktivně si všímat varovných signálů závislosti (v případě pocitu úzkosti, depresí nebo podrážděnosti, když sítě nevyužíváme – ihned jejich užívání omezit). Vyhledání odborné pomoci, pokud máme pocit, že nemáme užívání sítí pod kontrolou.[48]

[47] DOC. MGR. KOPECKÝ KAMIL PH.D. E - BEZPEČÍ. Rodiče, nepanikařte! Film V síti je sice syrový, ale bezpečnost dětí v online prostředí není těžké zabezpečit. Stačí se držet několika rad! [online]. [cit. 2024-02-29]. Dostupné z: https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1791-rodice-nepanikarte-film-v-siti-je-sice-syrovy-ale-bezpecnost-deti-v-online-prostredi-neni-tezke-zabezpecit-staci-se-drzet-nekolika-rad

[48] FINEFIFTY. Závislost na internetu a sociálních sítích: velké nebezpečí moderního světa [online]. [cit. 2024-02-29]. Dostupné z: https://fine50.cz/zavislost-na-internetu-a-socialnich-sitich-velke-nebezpeci-moderniho-sveta/

4 Trestná činnost páchána ve virtuálním prostředí

V souvislosti s vyjmenovanými bezpečnostními riziky může být též spáchané nemalé množství trestných činů podle v České republice platného trestního zákoníku. V této kapitole bude tak čtenář seznámen s nejzásadnějšími trestnými činy, které mohou být spáchány v rámci jednotlivých rizik z virtuálního prostředí.

Kyberšikana

§ 144 Účast na sebevraždě, § 145 Těžké ublížení na zdraví, § 146 Ublížení na zdraví, § 175 Vydírání, § 181 Poškození cizích práv, § 184 Pomluva, § 345 Křivé obvinění, § 352 Násilí proti skupině obyvatelů a proti jednotlivci, § 354 Nebezpečné pronásledování, § 355 Hanobení národa, rasy, etnické nebo jiné skupiny osob, § 404 Projev sympatií k hnutí směřujícímu k potlačování práv a svobod člověka[49]

Zneužití osobních údajů

§ 175 Vydírání, § 180 Neoprávněné nakládání s osobními údaji, § 209 Podvod, § 210 Pojistný podvod, § 211 Úvěrový podvod, § 230 Neoprávněný přístup k počítačovému systému a nosiči informací, § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat, § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti, § 234 Neoprávněné opatření, padělání a pozměnění platebního prostředku[50]

Dezinformace, fake news, hoaxy

§ 184 Pomluva, § 355 Hanobení národa, rasy, etnické nebo jiné skupiny osob, § 356 Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod, § 357 Šíření poplašné zprávy[51]

[49] Zákon č. 40/2009 Sb., trestní zákoník v posledním znění
[50] Tamtéž
[51] Tamtéž

Online predátoři a kybergrooming

§146 Ublížení na zdraví, § 171 Omezování osobní svobody, § 175 Vydírání, §185 Znásilnění, § 186 Sexuální nátlak, § 187 Pohlavní zneužití, §191 Šíření pornografie, § 192 Výroba a jiné nakládání s dětskou pornografií, § 193 Zneužití dítěte k výrobě pornografie, § 193a Účast na pornografickém představení, §193b Navazování nedovolených kontaktů s dítětem, § 201 Ohrožování výchovy dítěte, § 202 Svádění k pohlavnímu styku, § 353 Nebezpečné vyhrožování, § 354 Nebezpečné pronásledování[52]

Závislost na sociálních mediích

Vzhledem k povaze tohoto rizika, a to konkrétně, že závislost vzniká v člověku samotném a v tomto případě bez zavinění konkrétního agresora, nelze toto rizika žádným způsobem kriminalizovat.

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

II. Praktická část

5 Kazuistiky rizik na sociálních sítích

Cílem praktické části této práce je pomocí položízených rozhovorů zpracovat a přednést reálné případy (kazuistiky) těch, kteří se ve svém životě již se zmíněnými bezpečnostními riziky setkali.

V každé kazuistice nejdříve popíši celou událost a poté uvedu, jaké problémy z události vyvstaly pro oběť. Závěrem jednotlivých kazuistik bude uvedení řešení, kterým se událost uzavřela.

První kazuistika je o chlapci, který byl terčem kyberšikany. Druhá kazuistika se týká dívky, která se stala obětí kybergroomingu. Následující kazuistika představuje příběh o seniorovi, který se stal obětí dezinformací. Čtvrtá kazuistika bude pojednávat o osobě, které byly zneužity osobní údaje, a poslední rozhovor ukáže, jak velkým problémem může být závislost na sociálních mediích.

Vzhledem k citlivosti jednotlivých témat byla jména osob v kazuistikách změněna. Zároveň byly pozměněny nebo záměrně neuvedeny některé údaje, pomocí kterých by se daly osoby z kazuistik identifikovat (místa bydliště, jména přátel, rodičů, jména institucí a další).

5.1 Kazuistika č. 1
Kyberšikana ve školním prostředí

Oběť: Velmi chytrý, tichý a spíše introvertní 16letý student střední školy, který se zajímá především o informatiku a výpočetní vědy. Má pouze malý okruh blízkých přátel, se kterými se věnuje turistice a občas s nimi chodí do posilovny. Pro účely této práce bude představen pod jménem Karel.

Popis události: K celé události došlo asi před rokem, když Karel přišel ze základní školy na střední školu. Karel má ze základní školy partu 4 kamarádů, kteří sdílejí stejné záliby a jsou mu oporou, ale když šel na střední školu, tak každý z jeho kamarádů šel na jinou školu, kdy pouze jeden z jeho kamarádů šel na stejnou školu, a do stejné třídy jako on. Karel byl nadšený, že alespoň jeden jeho kamarád šel s ním a vše bylo asi půl roku v pořádku. Karlův kamarád, který s ním ze základní školy šel na střední školu (pro tuto práci jménem Petr) se chtěl, ale cítit více přijímaný novým kolektivem, a proto, když si noví spolužáci Karla začali dobírat kvůli stylu jeho oblékání, tak se k nim Petr přidal. Zpočátku šlo pouze o různé posměšky a schválnosti, ale vše vyvrcholilo tím, že když Karel o jedné přestávce jedl jogurt, tak k němu přistoupil Petr, jogurt mu vzal, vyklopil mu ho na hlavu a tričko a začal vykřikovat, že Karel masturbuje ve škole, ať se všichni podívají, že je to pravda. V tu chvíli se Karlovi většina spolužáků začala znovu posmívat a Petra tak přijali mezi sebe. Po tomto se Karel sebral a odešel domů, kde řekl, že mu není dobře. Ve večerních hodinách se podíval na svůj uživatelský profil na Facebooku, kde si Karel všiml, že k jeho profilu sdílel Petr video z popsané přestávky. Video se začalo rychle šířit po celé škole, vznikaly různé koláže, předělávky a vtipy týkající se Karlovy osoby. Spolužáci také začali vytvářet různé profily odkazující na Karla a masturbaci ve škole, přičemž mu ho obtěžovali nevyžádanými zprávami a uráželi ho.

Vzniklé problémy: Kvůli strachu z dalšího šikanování se začal Karel vyhýbat škole i svým kamarádům ze základní školy a zůstával nejraději doma, v pohodlí svého pokoje. Byl více podrážděný a uzavřený. Nad to vše začal mít problémy se spánkem. Také se mu zhoršily do té doby vynikající studijní výsledky.

Uzavření události: Když se o chování Petra a Karlových problémech dozvěděli jejich kamarádi ze základní školy, tak přišli společně za Karlem domů. Podpořili ho a řekli mu, že se s Petrem již dále nebaví ani oni. Karla to povzbudilo, opět se začlenil mezi své kamarády a o celé situaci informoval své rodiče, které rovněž požádal, aby to dále neřešili, protože by se situace mohla zhoršit s tím, že si vybral novou střední školu a tu dosavadní již navštěvovat nebude, přičemž si také smazal své sociální sítě, aby se už dále netrápil. Nyní Karel chodí na novou střední školu, kde je spokojený, která ve výsledku více vyhovuje jeho zálibám, a tedy jsou zde i podobně smýšlející spolužáci, mezi kterými má i nové kamarády, kteří se také seznámili s jeho partou přátel ze základní školy. S Petrem již od té doby neudržuje žádný kontakt.

5.2 Kazuistika č. 2
Online predátor

Oběť: Společenská, extrovertní 15letá studentka základní školy, trávící spoustu volného času sledováním sociálních sítí už asi od 11 let. Pro účely této práce bude představena pod jménem Tereza.

Popis události: K incidentu došlo přibližně před dvěma lety, když Tereze bylo 13 let. Tou dobou trávila Tereza spoustu času na sociálních sítích, a to především na platformě s názvem Instagram. Tato platforma slouží převážně ke sdílení fotografií, přičemž Tereza zde tou dobou sdílela skrze fotografie velkou část svého života, a to včetně různých míst, kde se zdržuje. U svého profilu neměla nastavené soukromí, což znamená, že jakýkoliv uživatelský profil může vidět její příspěvky (fotografie). Již si nevzpomíná na jméno profilu, ale tento začal její fotografie označovat jako „to se mi líbí“ (začal ji „dávat lajky“). Na uvedeném profilu se prezentoval mladý (15letý), hezky vypadající kluk. Tento skrze zprávy Terezu oslovil. Zpočátku si spolu psali, skrze textová okna na Instagramu, kdy kluk uváděl, že bydlí ve stejném městě jako ona a zajímal se o Terezin život, přičemž s ní sdílel i své "tajemství". Byl hodný, milý, uváděl podobné zájmy, jako má Tereza, také psal, že má stejné názory apod. Postupně začal do jejich konverzací přidávat

různé sexuální narážky, ale protože se Tereze líbil, tak ta to nijak neřešila a občas také nějakou narážkou odpověděla.

Toto trvalo asi měsíc, načež neznámý „kluk“ Tereze řekl, že by si spolu mohli zavolat skrze videohovor, kdy ona souhlasila. Během hovoru ji řekl, že mu nějak nefunguje videokamera, ani mikrofon a nemůže to zprovoznit, tak že bude psát a ona může mluvit. Po asi 5 minutách tohoto videohovoru ji začal vybízet k tomu, aby se před ním svlékala a prováděla různé intimnosti, a to i přesto, že mu Tereza již předtím několikrát říkala, že je jí 13 let. To naštěstí Tereze už přišlo zvláštní, protože si vzpomněla, že na toto závadové jednání upozorňovali policisté, kteří u nich ve škole měli asi rok předtím přednášku týkající se bezpečnosti na internetu.

Vzniklé problémy: Tereza se po nějakou dobu po této události bála chodit sama městem a neustále se rozhlížela, zda není sledována. Rovněž do dnešního dne nedůvěřuje cizím lidem, což ji mnohdy znepříjemňuje život nebo navazování nových vztahů s jejími vrstevníky.

Uzavření události: Poté, co si Tereza uvědomila, že není vše v pořádku, tak videohovor okamžitě ukončila a ihned odstranila svůj účet na platformě Instagram (dnes má již nový). Zároveň účet „kluka“ nahlásila správci sítě a o celé události obeznámila své rodiče. Společně s rodiči vše oznámila policii, které se v tomto případě podařilo neznámého predátora ztotožnit a dovést k odpovědnosti (nebylo blíže specifikováno).

5.3 Kazuistika č. 3
Podlehnutí dezinformacím

Oběť: Vzdělaný, ovdovělý senior, 79letý senior, který se snaží držet krok s dnešní uspěchanou dobou, a proto se stále zdokonaluje v ovládání svého počítače a čte si různé světové novinky. Muž většinu času tráví sám doma, přičemž jeho děti a vnoučata ho občasně navštěvují. Pro účely této práce bude pojmenován Josef.

Popis události: Tato událost se začala odehrávat v době, kdy ve světě vypukla pandemie Covid-19, a to v roce 2020. Josef, který se stále snažil držet krok s dnešní dobou, se dostal k článku pojednávajícím o této nemoci a vyvíjeném očkování, který byl uveřejněn na nejmenované webové stránce (pozn. web je ministerstvem vnitra ČR zařazen na seznamu dezinformačních internetových stránek). V tomto článku bylo uváděno, že „Covid-19 je pouze propaganda novodobé vládnoucí vrstvy a vyvíjená vakcína obsahuje nanočipy vytvořené Elonem Muskem, aby mohlo být obyvatelstvo ovládáno." Protože podobných článků bylo publikováno několik, a to i v cizím jazyce a byly zde přiloženy fotografie jako „důkazy", tak Josef článkům uvěřil.

Vzniklé problémy: Josef začal být nepřátelský vůči své rodině, která se ho snažila přesvědčit, že tyto články se nezakládají na pravdě, a to i podloženými informacemi. Senior se dále uchýlil k získávání nových informací ze světa pouze prostřednictvím dezinformačního webu, kam rovněž měsíčně zasílal finanční částky, aby „podpořil odkrývání pravdy" (jak tento web sám uváděl).

Uzavření události: Přestože měl Josef zdravotní problémy týkající se dýchací soustavy, tak očkování odmítal. V roce 2021 byl Josef hospitalizován v nemocnici po proděláni onemocnění Covid-19, kde o několik dní později zemřel na následky plicní fibrózy.

Pozn. Tato kazuistika byla zprostředkována skrze Josefova rodinného příslušníka.

5.4 Kazuistika č. 4
Zneužití osobních údajů

Oběť: Vysokoškolsky vzdělaná, 40letá žena pracující jako účetní v soukromé firmě. Žena čas od času prodává své přebytečné věci skrze různé inzerce na internetu. Pro účely této práce bude představena jako Lenka.

Popis události: Přibližně v prosinci roku 2023 Lenka inzerovala skrze platformu Facebook – Marketplace (sekce na platformě Facebook, kde lze inzerovat různé věci k prodeji) svůj starý mobilní telefon za částku 2 500 Kč.

Na tuto inzerci se ji ozvala osoba přes sociální síť Messenger (k Facebooku přidružená síť určena pro psaní zpráv mezi lidmi z Facebooku). Jméno osoby bylo napsáno azbukou, přičemž tato osoba Lence napsala, že by měla o mobilní telefon zájem. Přestože profil byl pojmenován azbukou, tak osoba psala plynule českým jazykem. Lenka se s osobou domluvila na prodeji mobilního telefonu, přičemž osoba po Lence požadovala, aby jí inzerovaný mobilní telefon zaslala na dobírku skrze Zásilkovnu (společnost zabývající se dopravou zásilek) s tím, že kurýr by si pro zboží přijel. Následně neznámá osoba Lence zaslala odkaz na webovou stránku, jenž měl v názvu "zásilkovna". Po otevření odkazu byla na webové stránce Lenka vyzvána k tomu, aby vyplnila své jméno, příjmení a datum narození. Dále Lenka zvolila svou banku a poté byla vyzvána, aby vyplnila přihlašovací jméno a heslo od svého internetového bankovnictví. Poté Lenka vyplnila všechny své údaje k platební kartě, a to šestnáctimístný kód, datum platnosti karty a třímístný CVV kód. Když Lenka vše vyplnila, napsala neznámé osobě, že vše zadala podle instrukcí, načež jí bylo zasláno potvrzení, že je vše v pořádku a nyní má čekat na slíbenou částku ve výši 2 500,- Kč a na kurýra, který si pro mobilní telefon přijede.

Vzniklé problémy: Následujícího dne se Lenka chtěla přihlásit do svého internetového bankovnictví, což ji však bylo zamítnuto, a proto kontaktovala svou banku, kde ji bylo sděleno, že na jejím účtu detekovali podezřelé transakce, a proto byl její účet zablokován. Na pobočce banky Lenka zjistila, že toho dne, kdy zadala své údaje z platební karty na podvodnou webovou stránku, tak ji z účtu byly zadány dvě transakce a to v celkové výši 45000,- Kč, přičemž obě byly ve prospěch v zahraničí vedených „internetových peněženek“, odkud byly následně přeposlány na různé zahraniční účty.

Uzavření události: Poté, co se Lenka dozvěděla o tom, že její osobní údaje z platební karty byly zneužity, vše oznámila na nejbližší oddělení PČR. Celá věc byla zaevidován, ale vzhledem k tomu, že byly peníze již rozeslané na různé zahraniční účty, nepodařilo se dohledat pachatele a banka nemohla transakci pozastavit. Lenka tak přišla o svých našetřených 45000,- Kč.

5.5 Kazuistika č. 5
Závislost na sociálních sítích

Oběť: Vysokoškolsky vzdělaná 25letá žena, pracující jako vedoucí marketingu v soukromé společnosti. Od jejich 12ti let, kdy se poprvé připojila na platformu Facebook, zde trávila stále více a více času. Dnes postupuje s dobou, a přestože Facebook v posledních letech nemá takovou popularitu jako dříve, přesunul se její zájem směrem k novým trendům v oblasti sociálních sítí, jako jsou především platformy Instagram a TikTok. Pro účely této práce bude žena představena jako Eva.

Popis události: Jak je již výše uvedeno, Eva sociální sítě používá již asi od svých 12 let. Největší problém v souvislosti s jejich používáním začal v lednu roku 2023. Tou dobou procházela rozchodem po dlouholetém vztahu, kdy z důvodu „útěku od reality“ začala trávit ještě více času na sociálních sítích, než obvykle. Později začala na sociálních sítích sdílet také více svých fotografií a příspěvků, a to především na platformě Instagram. Zde neustále sledovala, kolik „lajků“ pod který příspěvek dostává a začínala se porovnávat s ostatními uživateli, kteří měli „lajků“ více. Protože neustále sledovala jiné profily, porovnávala se s nimi a sama se v online prostředí snažila získat co nejvíce pozornosti, začala sociální sítě sledovat i v práci a přestala se věnovat svým volnočasovým aktivitám. Prakticky přesunula veškerý svůj sociální život z reálného světa, do toho virtuálního.

Vzniklé problémy: Eva ve svém zaměstnání začala zanedbávat své pracovní úkoly. Dočasně ztratila několik svých známých z reálného života, protože se s nimi přestala scházet. Ztratila veškerý zájem o své volnočasové aktivity, jako byl běh, plavání a čtení knih. Dokonce se u ní projevily známky úzkosti v momentě, kdy ji například přišlo oznámení o aktivitě z Instagramu a ona jej nemohla ihned zkontrolovat nebo, když neměla dostatečné internetové spojení, aby se mohla sociálním sítím věnovat. Vzhledem k tomu, že stále sledovala upravované a profesionální fotografie některých uživatelů, začala mít pocit, že má nadváhu, což vedlo až k poruše příjmu potravy.

Uzavření události: Takto Eva žila asi půl roku, ale vše se začalo měnit, když shlédla dokument s názvem „Sociální dilema“ na platformě Netflix (služba, která sdílí seriály, filmy a dokumenty. V tomto dokumentu varují odborníci společnost před úskalími sociálních sítí, které oni sami tvořili. Eva si poté začala postupně uvědomovat, že její užívání sociálních sítí začalo být nejspíš problematické, a proto se snažila svou aktivitu zde omezit. Nicméně zjistila, že na tento problém a zejména na problém s příjmem potravy asi sama nestačí, a proto vyhledala pomoc kvalifikovaného psychiatra. S jeho pomocí začala Eva postupně svou aktivitu na sociálních sítích omezovat, začala si opět vážit sama sebe a znovu se začala věnovat svým kamarádům, práci a svým dřívějším zájmům. Dnes již Eva pomoc psychiatra nepotřebuje, ale sama přiznává, že jenom díky jeho pomoci a pomoci svých blízkých se mohla znovu „vrátit do reálného života“, své účty na sociálních sítích smazat a začít si více vážit sama sebe.

6 Správný postup a doporučení prevence

V této části práce bude proveden řízený rozhovor se specialistou prevence Policie České republiky prap. J. P. zařazeném na územním odboru Mladá Boleslav. Prap. J. P. byl se souhlasem obětí seznámen s kazuistikami uvedenými v přechozí kapitole. Výsledkem této kapitoly bude zhodnocení jednotlivých kazuistik, zejména popis případného chybného jednání oběti, představení správného postupu v případě vzniku některého z rizik a doporučení prevence u každého z nich. Kapitola bude zpracována formou otázek ze strany autora práce a odpovědí ze strany specialisty prevence prap. J. P.

6.1 Kyberšikana

Jste obeznámen s problematikou týkající se kyberšikany? Ano jsem. Jedná se o útoky agresora, které jsou realizovány pomocí informačních technologií, čímž se kyberšikana odlišuje od klasické šikany, která probíhá mimo informační technologie.

Byl jste seznámen s první kazuistikou této práce. Jak byste vyhodnotil jednání oběti? V jednání oběti je potřeba zdůraznit především to, že oběť svůj problém nechtěla s nikým řešit a vše si nechávala pro sebe, čímž došlo k upevnění „moci“ agresora nad obětí a agrese se dále stupňovala, až vygradovala v neúnosnou situaci, kterou však oběť dále odmítala řešit a namísto toho se uzavřela do sebe. Následkem toho všeho byl vznik několika zásadních problémů, které mohly přerůst ve značné psychické trauma nebýt přátel oběti, kteří se zachovali velmi pozitivně.

Jak by se tedy oběť v případě setkání s kyberšikanou měla zachovat podle vás? Obecně bych doporučil na šikanu neodpovídat vlastním agresivním chováním. Dále vše sdělit alespoň osobě, ve které má oběť oporu a důvěřuje ji, a to především proto, že oběť poté nemá pocit, že je na vše sama, a blízká osoba může poskytnout též velmi cenné rady. V nejlepším případě vše říct rodičům, pracovníkům školy nebo celou věc oznámit na nejbližším útvaru Policie ČR.

Mým dalším doporučením je uchovávat důkazy o tom, že ke kyberšikaně skutečně dochází, protože agresor často svou vinu odmítá a vše popírá. Taktéž lze u většiny

sociálních platforem nahlásit různé příspěvky nebo uživatelské profily jako „škodlivé“ nebo „urážlivé“, přičemž správci sítě učiní nezbytná opatření (smazání příspěvku nebo profilu).

Existuje nějaká prevence proti kyberšikaně? Ano určitě. V první řadě je důležité veřejnost a zejména mladé lidi informovat o tom, že kyberšikana je zásadní problém a také o tom, jak ji lze rozpoznat v jejích začátcích. Různé přednášky týkající se této hrozby by bezesporu měly být součástí vzdělávacího programu každého školského zařízení. Přednášky ve školách dělám i já sám nebo moji kolegové, pokud nás o to některá škola požádá, přičemž v rámci těchto přednášek zdůrazňujeme mimo jiné i problémy týkající se kyberšikany. Rovněž je důležité informovat veřejnost též skrze odborné články šířené i prostřednictvím médií a online zdrojů. Za další formu prevence lze též označit mechanismy jednotlivých sociálních sítí, které umožňují hlášení a řešení závadového chování svých uživatelů. U mladších osob lze též monitorovat jejich online chování „rodičovskou kontrolou“ (online mechanismus umožňující spravování účtů a ovládacích prvků těchto účtů, případně plný přístup k těmto účtům). Takovou obecnou prevencí proti útokům různých agresorů jsou existující a správně implementované právní předpisy, se kterými je důležité seznámit veřejnost, čímž u spousty jedinců dojde k vyvarování se závadovému jednání, neboť nestojí o žádné „problémy se zákonem“.

6.2 Online predátoři

Jste obeznámen s problematikou týkající se online predátorů? Ano, jedná se především o obtěžování osob pomocí informačních technologií, přičemž toto obtěžování má zpravidla sexuální podtext. Tato problematika je velmi vážným rizikem na sociálních sítích, a to především protože obětí bývají nejčastěji děti. Z tohoto důvodu je také většina těchto událostí řešena příslušnými útvary služby kriminální policie a vyšetřování (SKPV).

Byl jste seznámen s druhou kazuistikou této práce. Jak byste vyhodnotil jednání oběti? Chybou v tomto případě bylo především to, že oběť na sociální síti sdílela

velké množství svých osobních informací a zároveň neměla svůj profil nijak chráněný před „nezvanými návštěvníky“. Většina sítí totiž umožňuje nastavení si svého uživatelského profilu tak, aby osoba nesdílela své příspěvky s veřejností, ale pouze s účty, které osoba sama schválí. Nicméně bych určitě chtěl vyzdvihnout správnou reakci oběti v momentě, kdy byla vyzvána k intimnostem v rámci videohovoru a její následné postupy, kdy vše sdělila svým rodičům, a vše oznámili Policii ČR, aby nedošlo k dalším útokům tohoto agresora na jinou oběť.

Jak by se měla oběť v případě setkání s online predátorem zachovat podle vás? Při setkání s online predátorem doporučuji ihned ukončit veškerý kontakt s touto osobou, aby nedošlo ke vzniku závažnějších problémů. Stejně jako u kyberšikany pak doporučuji vše sdělit blízké osobě, rodičům, nebo pedagogickým pracovníkům. Veškerou komunikaci zálohovat stejně jako informace, které by mohly vést ke ztotožnění pachatele a následně vše ihned oznámit na nejbližším útvaru Policie ČR. Případně lze kontaktovat poradnu E-Bezpečí nebo Linku bezpečí. Uživatelské profily predátorů lze taktéž oznámit správcům jednotlivých sociálních sítí.

Jaká je prevence v boji proti online predátorům? Stejně jako u kyberšikany je velmi důležité o rizicích online predátorů informovat zejména dospívající osoby a děti, protože ti jsou nejvíce ohroženou skupinou, co se týče této hrozby. Vzhledem k tomu, že v tomto případě vznikají velmi vážné problémy, je podstatné osobám uvést takové informace, aby riziko rozpoznali již v začátcích. Různé přednášky týkající se této hrozby by měly být součástí vzdělávacího programu každého školského zařízení a znovu zdůrazňuji, že i já sám nebo moji kolegové tuto „osvětu“ ve školských zařízeních realizujeme a jsem velmi rád, že naše prevence měla v tomto případě takový efekt a nedošlo tak ke vzniku závažnějšího problému. Společnost dále musí být informována o tom, že pokud ke vzniku nějakého problému dojde, je velmi důležité nebát se věc řešit s příslušnými orgány nebo svými blízkými. Dospělé osoby pracující s dětmi a též jejich rodiče, by měli být taktéž s celou problematikou obeznámeni, aby mohli ohroženým osobám poskytnout potřebnou pomoc. Prevence je též prováděna formou odborných článků, přičemž v tomto odvětví odvádí výbornou práci webová stránka E-Bezpečí a kybergrooming. Dalším zdrojem prevence mohou být filmy a seriály

pojednávající o této problematice. Zde bych zmínil především český dokumentární film s názvem „V síti“, který je jakýmsi experimentem a mladým lidem přibližuje problematiku týkající se online predátorů, a to v takovém podání, které je jim v dnešní době bližší, než čtení odborné literatury. Za další formu prevence bych označil mechanismy jednotlivých sociálních sítí, které umožňují hlášení a řešení závadového chování svých uživatelů a nastavení si svého soukromí, tedy nastavení toho, co o nás můžou neznámé osoby na sociálních sítích zjistit. Znovu lze též monitorovat online chování svých dětí pomocí „rodičovské kontroly“. V tomto případě je velmi důležité, aby případní agresoři byli od svého jednání odrazováni, k čemuž slouží opět právní předpisy. Důležité je však ukládání vyšších trestních sazeb pachatelům, kteří jsou dopadeni, aby mohla být společnost adekvátně chráněna a cítila potřebnou podporu veřejnosti v této problematice spojenou s intimitou obětí.

V tomto ohledu bych chtěl zdůraznit, že existuje také preventivní projekt s názvem Tvoje cesta onlinem, který je vybudován společnou prací Policie ČR a bankou ČSOB a jehož výsledkem jsou návody, jak vést prevenci online kriminality páchané ve vztahu k dětem a rodičům.

6.3 Šíření dezinformací

Jste obeznámen s problematikou týkající se šíření dezinformací? S touto problematikou nejsem seznámen do detailů, protože se ji tolik nevěnuji. Obecné informace k této hrozbě však mám a mohu tak obecně odpovědět na otázky, které mi jsou kladeny. Obecně lze říci, že dezinformace jsou informace, které však nejsou pravdivé, ale záměrně jsou jako pravdivé šířeny ve společnosti. Jejich účelem je ovlivnit názory a myšlení společnosti.

Byl jste seznámen se třetí kazuistikou této práce. Jak byste vyhodnotil jednání oběti v tomto případě? Zde bohužel nelze říci, že by se oběť zachovala alespoň nějakým způsobem správně.

Chybné je především to, že oběť odmítla naslouchat hlasu svých blízkých, zarputile byl přesvědčený o tom, že právě on má pravdu, což také vedlo k tomu, že odmítal jiné zdroje, ze kterých by mohl poznatky čerpat.

Další obrovskou chybou bylo zasílání finančních částek autorům této webové stránky, protože je tak podporována jejich činnost a tím i další šíření dezinformací.

Jak by se měla společnost chovat v souvislosti se dezinformacemi? Přestože online prostředí může být velmi dobrým pomocníkem a velmi rychle šíří zprávy z různých koutů světa, tak ne vždycky jsou veškeré informace založeny na skutečnostech. Obecně bych doporučil, aby každá informace z online prostředí byla prověřena několik spolehlivými zdroji. Na webových stránkách Ministerstva vnitra ČR je snadno dohledatelný seznam dezinformačních internetových stránek, což je také dobré vodítko k tomu, že informace pocházející z těchto stránek nemusejí být vždy pravdivé. Dále bych zdůraznil, aby se každý neupínal jen na „svou pravdu“ a snažil se vyslechnout i rady a názory ostatních, protože mýlit se může každý z nás.

Jak lze dezinformacím předcházet? Řekl bych, že důležité je informovat veřejnost o tom, jak mohou dezinformace rozpoznávat, a to především skrze sociální sítě nebo média. Rovněž je velmi důležité zjištěné informace řádně ověřovat, jak jsem již uváděl v předchozí odpovědi a určitě je dále nešířit, protože ne každý dezinformaci dokáže rozpoznat. Velmi kladně také cením přístup většiny sociálních sítí, které se snaží odstraňováním závadových příspěvků nebo uživatelských profilů zredukovat výskyt dezinformací v rámci svého online prostředí.

6.4 Zneužití osobních údajů

Jste obeznámen s problematikou týkající se zneužití osobních údajů? Ano jsem a řekl bych, že v současnosti je podvodné jednání spojeno se zneužitím osobních údajů asi nejčastější hrozbou, která se v souvislosti se sociálními sítěmi objevuje. Jde především o jednání, kdy pachatel naváže kontakt s obětí a vyláká z ní údaje k platební kartě nebo bankovnímu účtu a tyto následně zneužije k odčerpání finanční hotovosti zpravidla na zahraniční účty nebo internetové peněženky.

Byl jste seznámen se čtvrtou kazuistikou této práce. Jak byste vyhodnotil jednání oběti v tomto případě? Bohužel tato forma podvodu byla svého času velmi populární a alespoň zpočátku dost úspěšná.

Internetové stránky přepravní společnosti byly velmi zdařilé a v obětech to skutečně vzbuzovalo důvěru, že se jedná o známou společnost, která zásilky skutečně doručuje a nepojali tak žádné podezření, že by mohlo jednat o podvod. Policie ČR o tomto podvodném jednání celou společnost velmi rychle informovala skrze masová média, nicméně vzhledem propracovanosti tohoto jednání stále k podvodům docházelo, dokud toto povědomí sami oběti nerozšířily mezi svými blízkými. Jednání oběti bych tak označil za chybné snad jen v tom, že při zadávání svých osobních údajů nebyla obezřetná a podezřívavá.

Jak by se podle vás měla oběť zneužití osobních údajů zachovat? Důležité je především rozpoznat, jaká činnost by v online prostředí mohla být riziková a poté k ní také tak přistupovat. Obecně bych doporučil, že pokud někam v online prostředí zadáváme své osobní údaje, měli bychom být velmi obezřetní a při každé takové činnosti být spíše podezřívaví. V případě, že ke zneužití osobních údajů dojde, oběť by prvně měla zablokovat veškeré své napadené účty, aby k dalšímu zneužívání již nedocházelo. Dále by tuto zkušenost neměla nechávat sama pro sebe, ale měla by to sdílet s co největším okruhem svých blízkých a především celou věc okamžitě oznámit policejnímu orgánu k provedení dalších potřebných opatření, neboť při rychlém jednání s bankovními společnostmi a policejními orgány lze odčerpání finančních prostředků pozastavit a zamezit tak značným škodám.

Jaká je prevence v oblasti zneužívání osobních údajů? V souvislosti s prevencí je nutné zdůraznit, že způsoby, jakými ke zneužití osobních údajů dochází, se neustále vyvíjí a zlepšují. Zpravidla dojde k několika útokům, než je postup podvodu odhalen a rozšířen v povědomí společnosti, což bývá velmi problematické. Obecně lze však říci, že nejdůležitější prevencí v rámci této hrozby je rychlá reakce policejního orgánu vedoucí k rozpoznání podvodného jednání a následné rozšíření informace ve společnosti tak, aby se ohrožená skupina co nejvíce zúžila.

Další důležitou složkou prevence v této oblasti je obezřetnost při otevírání odkazů, podezřívavost při zadávání osobních údajů kdekoliv v online prostředí a aktivní zjišťování nových forem podvodů. Za nejzákladnější způsob obecné ochrany osobních údajů lze nejspíš označit „nastavení soukromí“, dvoufázová autentizace,

používání silných hesel a případně udržování aktualizovaného softwaru tam, kde je to v online prostředí možné.

6.5 Závislost na sociálních médiích

Jste obeznámen s problematikou týkající se závislosti na sociálních sítích? Musím přiznat, že s touto problematikou jsem seznámen pouze teoreticky a zatím jsem se s tímto problémem nesetkal v reálném životě. Podle všeobecné teorie je však tato závislost stejně srovnatelná s jinými a skutečně se může objevit, pokud člověk sociální média používá neuváženě.

Byl jste seznámen s pátou kazuistikou této práce. Jak byste vyhodnotil celou tuto událost? Jakákoliv osoba může spadnout do různých závislostí zejména, když jsou jeho dosavadní „zájmy“ na hranici rizikového chování. Dost často pak bývá jakýmsi impulsem nějaká nepředvídatelná, silně emocionální událost. V rámci tohoto příběhu mohl být velmi pravděpodobně tímto impulsem uváděný rozpad dlouholetého vztahu a s tím spojený „útěk od reality“, což ve výsledku způsobilo opravdový problém. Nicméně bych velmi kladně vyhodnotil, že si v tomto případě oběť svůj problém sama uvědomila a vyhledala odbornou pomoc, neboť toto je velmi důležité při zvládání jakékoliv závislosti.

Jak by se podle vás měla závislá osoba zachovat? Úplně nejdůležitější je rozpoznání, že má osoba problém. Rozpoznat to může sama závislá osoba nebo její okolí. Pokud to osoba pozná sama, tak je zásadní, aby měla odhodlání se závislostí chtít bojovat. Když závislost u osoby rozpozná její okolí, je zapotřebí, aby se závislou osobou co nejcitlivěji promluvili (pomohli ji tak důsledky svého chování), upřímně vyjádřili své obavy o ní a poskytli ji porozumění a podporu. V některých případech lze se závislostí bojovat za pomocí nastavení si hranic (v tomto případě hranic používání sociálních sítí) a též za pomocí alternativních aktivit, které mohou odvést pozornost od závislosti. Pokud selžou veškeré snahy o zvládnutí závislosti vlastními silami, je zapotřebí vyhledat pomoc odborníka (adiktologické ambulance a psychologické ambulance či psychiatrické ambulance). Všechna tato obecná doporučení lze aplikovat i právě na používání sociálních sítí.

Jaká je prevence v oblasti závislosti na sociálních médiích? Důležitou prevencí v této oblasti je informování společnosti, že k tomto druhu závislosti může skutečně dojít. Já a spousta mých kolegů na tento problém v rámci svých přednášek upozorňujeme, nicméně se zatím nejedná o standard a o tomto druhu závislosti se moc nemluví. Dokonce samotná společnost tuto závislost nebere zatím nijak vážně, ale v příběhu oběti je jasně vidět, že z této hrozby mohou vyvstat i jiné problémy, jakým byla právě uvedená porucha příjmu potravy. Po uvědomění si, že problémy mohou skutečně nastat je zásadní si stanovit hranice v užívání sítí, a to může být stanovení si času, jaký chceme v online prostředí trávit a striktní dodržování tohoto nastavení. Další prevencí před vznikem závislosti na sociálních sítích je bezesporu vypnutí notifikací (upozornění), které nás neustále nutí se k dané sociální síti připojovat tím, že nás upozorňují na aktivity ostatních uživatelů a vybízejí nás ke sledování těchto aktivit a k připojení se k nim. Jako poslední bod bych uvedl, že mít stabilní sociální život v reálném prostředí namísto toho virtuálního může být také velmi rozhodující.

6.6 Doplňující otázky

Jaká jsou podle vás obecná doporučení při pohybu na sociálních sítích? Obecně vždy doporučuji používat silná hesla ke svým účtům, být obezřetný a do jisté míry podezíravý. Dále slepě nedůvěřovat veškerým přečteným informacím, které bychom si měli vždy ověřit. Také nedůvěřovat všem uživatelům, že jsou tím, čím tvrdí, že jsou a při seznamování skrze sociální sítě být velmi opatrný. Mé poslední doporučení je, aby si lidé udržovali sociální vazby v reálném životě a nepřesouvali je pouze do toho virtuálního, aby na sociálních sítích nesdíleli veškerý obsah svého života a netrávili zde veškerý svůj volný čas.

Která věková skupina je v souvislosti s bezpečnostními hrozbami na sociálních sítích tou nejvíce ohroženou? To se může lišit v závislosti na tom, o jaké hrozbě mluvíme. Nicméně pokud se budeme držet hrozeb, o kterých pojednává tato práce, tak nejvíce ohroženou skupinou jsou děti a mladí dospělí, kteří v online prostředí tráví opravdu hodně svého volného času.

Ovšem je nutné zdůraznit, že zneužití osobních údajů a s tím spojené podvodné jednání bývá spíše zaměřeno na dospělou část naší populace, neboť tato již disponuje finančními prostředky, jejichž získání je cílem útočníků. Co se týká dezinformací, zde je nejvíce ohroženou skupinou starší obyvatelstvo, neboť většina z nich má zájem na získávání informací pomocí nových technologií, ale nedokáží již tyto informace správně vyhodnotit a důvěřují téměř všemu, co se v online prostředí dozvědí a poté už jen záleží na tom, z jakých zdrojů zrovna čerpají.

Jaká hrozba je v současnosti na sociálních sítích nejvíce rozšířená? Nejvíce rozšířenou hrozbou je dle mých dostupných informací bezpochyby zneužití osobních údajů spojené s následným podvodným jednáním. Další velmi rozšířenou hrozbou je kyberšikana mezi dětmi a dospívajícími a poté kybergrooming. Nicméně bych rád podotknul, že kazuistiky, které jsem v rámci této práce četl, reflektují právě ty hrozby online prostředí, které mezi všemi ostatními dominují.

Jaká hrozba je tou nejzávažnější? Nejzávažnější hrozbou je zcela jistě kybergrooming. Tato hrozba se totiž týká nejmladší části naší populace a vzhledem k tomu, že je spojena s útokem na intimitu osob, může zanechat hluboké psychické problémy, které následně mohou přetrvávat po celý život oběti. Nehledě na to, že je touto hrozbou narušen řádný vývoj dítěte.

Je podle vás prevence v České republice dostačující? Řekl bych, že je v této oblasti odváděna výborná práce, a to jak ze strany Policie ČR, tak různých dalších státních a nestátních organizací. Menší nedostatky spatřuji v oblasti vzdělávání uživatelů a ve využití nových technologií, jako je umělá inteligence. S jistotou lze říci, že prevence se neustále vyvíjí a v dnešní době je úroveň o dost lepší, než tomu bývalo v dřívějších dobách. Musíme však pamatovat na to, že vždy je prostor pro zlepšení a prevence by se měla neustále vyvíjet podle aktuálních trendů.

Závěr

Z celé této práce je patrné, že bezpečnostní rizika jsou na sociálních sítích velmi rozšířenou problematikou. I když sociální sítě byly vytvořeny zejména za účelem propojení jejich uživatelů, nelze jim odepřít též jejich stinnou stránku spočívající právě v tom, že se rovněž staly „úrodnou půdou“ pro vzestup, do té doby neznalých hrozeb.

Z teoretické části této práce též vyplývá, že nejzávažnější z těchto hrozeb je kybergrooming, což bylo v praktické části potvrzeno také specialistou prevence z řad Policie ČR. Nicméně je nutné pamatovat na to, že i další hrozby, jako je kyberšikana, zneužití osobních dat, šíření dezinformací a závislost na sociálních sítích, o kterých tato práce pojednává jsou též velmi závažné.

V rámci teoretické části této práce byly čtenáři představeny ty nejvíce rozšířené hrozby na sociálních sítích, a to „kyberšikana“, „online predátoři a s nimi spojený kybergrooming“, „dezinformace, „fake news a hoaxy“, „zneužití osobních dat“ a „závislost na sociálních médiích“. Že se jedná o ty nejvíce rozšířené bylo v praktické části této práce též potvrzeno specialistou prevence. Toto tvrzení je dále podpořeno tím, že ke každé uvedené hrozbě bylo možné zpracovat odpovídající kazuistiku.

Co se týče hrozbami na sociálních sítích nejohroženější skupiny, zde jsme rovněž došli ke shodě v teoretické části práce a té praktické. Z obou částí práce vyplývá, že nejohroženější skupinou jsou děti a dospívající, kteří sociální sítě využívají nejvíce. Je však nutné pamatovat na to, že ohrožené skupiny se mohou lišit v závislosti na dané hrozbě, což je též uvedeno v teoretické části a potvrzeno v té praktické (vyplývá to z jednotlivých kazuistik a též z rozhovoru s prap. J.P.).

Nejdůležitější částí této problematiky je však prevence. Odborné poznatky prap. J. P. v praktické části práce se v zásadě shodují s poznatky, které jsou uvedeny v části teoretické.

V oblasti prevence bych rád poukázal na dvě složky této problematiky, kde prap. J. P. spatřuje mírné nedostatky. Těmito složkami jsou vzdělávání uživatelů a využití nových technologií.

Vzdělávání uživatelů by mohlo být zlepšeno zejména zvýšením povědomí o bezpečnostních hrozbách, které ohrožují mladší generaci, a to jak mezi mladší generací, tak mezi jejich rodiči. Z celé práce vyplývá, že mezi největší hrozby pro mladší generaci patří kyberšikana, online predátoři a závislost na sociálních sítích. Na základě zjištěných poznatků je zřejmé, že mladí lidé spoustu svého času tráví sledováním influencerů (osobnosti známé na sociálních sítích). Tito influenceři by tak mohli být na základě spolupráce s vládou využiti k osvětě mladé generace, a to především přijatelnou a nenásilnou formou pro tuto generaci. Rovněž by bylo možné prvky prevence implementovat do videoher, seriálů a filmů, neboť tyto jsou též ve velké oblibě u mladší generace. Jednotlivé sociální sítě by také mohli vytvořit krátké „průvodce“, které by musel shlédnout každý nově zaregistrovaný uživatel a též by mohli pravidelně informovat o aktuálních hrozbách (například při nových podvodných taktikách útočníků). Pomocí influencerů, videoher, filmů a seriálů by bylo rovněž možné sdílet reálné zkušenosti lidí, kteří se již obětmi některé z hrozby staly, pokud by jim nevadilo svůj příběh sdílet s veřejností.

Na základě **nových technologií** by mohly sociální sítě využívat zejména strojového učení a umělé inteligence k identifikaci a odstraňování závadových aspektů online prostředí. Pomocí umělé inteligence by mohly být odhalovány hrozby jako jsou spam, nenávistné projevy, dezinformace, kyberšikana, podvodné emaily a weby. Dalším krokem ke zlepšení bezpečnosti (zejména k zabránění zneužití osobních údajů) by mohl být rozvoj silnějších bezpečnostních funkcí, jako je více faktorová autentizace a šifrování end-to-end (zpráva odesílaná chatovací aplikací se „zašifruje“, projde internetem a „dešifruje“ se až u příjemce). Tyto funkce jsou již některými sociálními sítěmi implementovány a slouží zejména k ochraně uživatelských účtů a dat, nicméně stále nejsou tolik rozšířeny.

Co se prevence týká, tak z celé práce vyplývá, že v této problematice je nejdůležitější osvěta společnosti, obezřetnost při pohybu v online prostředí, ověřování si zjištěných informací z kvalitních zdrojů, používat nejvíce účinné bezpečnostní funkce a sociální sítě využívat s mírou.

Seznam použité literatury

Monografie:

1. ČERNÁ, Alena. Kyberšikana: průvodce novým fenoménem. Psyché (Grada). Praha: Grada, 2013. ISBN 9788024745770.
2. ECKERTOVÁ, Lenka a DOČEKAL, Daniel. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. Brno: Computer Press, 2013. ISBN 9788025138045.
3. HULANOVÁ, Lenka. Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality. Praha: Triton, 2012. ISBN 978-80-7387-545-9.
4. KIRKPATRICK, David. Pod vlivem Facebooku: příběh z nitra společnosti, která spojuje svět. Brno: Computer Press, 2011. ISBN 9788025135730.
5. KOHOUT, Roman a KARCHŇÁK, Radek. Bezpečnost v online prostředí. Karlovy Vary: Biblio Karlovy Vary, 2016. ISBN 978-80-260-9543-9.
6. KOLOUCH, Jan. CyberCrime. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7.
7. KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.
8. LÉVY, Pierre. Kyberkultura: zpráva pro Radu Evropy v rámci projektu "Nové technologie: kulturní spolupráce a komunikace". V Praze: Karolinum, 2000. ISBN 80-246-0109-5.
9. MARTÍNEK, Zdeněk. Agresivita a kriminalita školní mládeže. 2., aktualizované a rozšířené vydání. Praha: Grada, 2015. Pedagogika (Grada). ISBN 978-80-247-5309-6.
10. ŠMAHAJ, Jan. Kyberšikana jako společenský problém: Cyberbullying as a social problem. Olomouc: Univerzita Palackého v Olomouci, 2014. ISBN 978-80-244-4227-3.

Zákonná úprava:

1. Zákon č. 40/2009 Sb., trestní zákoník v posledním znění

2. Zákona č. 101/2000 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) v posledním znění

Webové stránky a elektronické zdroje:

1. CZ.NIC. Jak na internet: Historie internetu [online]. [cit. 2024-02-29]. Dostupné z: https://www.jaknainternet.cz/page/1205/historie-internetu/
2. CZ.NIC. Nebojte se internetu [online]. [cit. 2024-02-29]. Dostupné z: https://www.nebojteseinternetu.cz/page/3396/socialni-site/
3. DENÍK VEKTOR. Informační technologie, umělá inteligence a ekonomika [online]. [cit. 2024-02-29]. Dostupné z: https://www.denikvektor.cz/ai/informacni-technologie-umela-inteligence-a-ekonomika-2373.html
4. DOC. MGR. KOPECKÝ KAMIL PH.D. E - BEZPEČÍ. Rodiče, nepanikařte! Film V síti je sice syrový, ale bezpečnost dětí v online prostředí není těžké zabezpečit. Stačí se držet několika rad! [online]. [cit. 2024-02-29]. Dostupné z: https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1791-rodice-nepanikarte-film-v-siti-je-sice-syrovy-ale-bezpecnost-deti-v-online-prostredi-neni-tezke-zabezpecit-staci-se-drzet-nekolika-rad
5. E - BEZPEČÍ. Co je to vlastně ten hoax, dezinformace, misinformace nebo třeba fake news? Čím se tyto termíny liší a co mají společného? [online]. [cit. 2024-02-29]. Dostupné z: https://www.e-bezpeci.cz/index.php/clanky-komentare/2864-co-je-to-vlastne-ten-hoax-dezinformace-misinformace-nebo-treba-fake-news-cim-se-tyto-terminy-lisi-a-co-maji-spolecneho
6. ESTUDOVNA. Vzdělávání po internetu [online]. [cit. 2024-02-29]. Dostupné z: https://www.estudovna.cz/cz/co-je-e-learning-vzdelavani-po-internetu95.html

7. FINEFIFTY. Závislost na internetu a sociálních sítích: velké nebezpečí moderního světa [online]. [cit. 2024-02-29]. Dostupné z: https://fine50.cz/zavislost-na-internetu-a-socialnich-sitich-velke-nebezpeci-moderniho-sveta/
8. INTERNETEM BEZPEČNĚ. Digitální stopa [online]. [cit. 2024-02-29]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/
9. INTERNETEM BEZPEČNĚ. Sociální sítě [online]. [cit. 2024-02-29]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/socialni-media/socialni-site/
10. KRYTOLAND. Nejpoužívanější sociální sítě v České republice [online]. [cit. 2024-02-29]. Dostupné z: https://www.krytoland.cz/clanek-nejpouzivanejsi-socialni-site-v-ceske-republice
11. KYBERGROOMING. KYBERGROOMING rizikové seznamování v online prostředí [online]. [cit. 2024-02-29]. Dostupné z: https://www.kybergrooming.cz
12. LIFELOCK BY NORTON. Who Are the Biggest Targets for Identity Theft? [online]. [cit. 2024-02-29]. Dostupné z: https://lifelock.norton.com/learn/identity-theft-resources/identity-theft-targets
13. MARYVILLE UNIVERSITY. The Evolution of Social Media: How Did It Begin, and Where Could It Go Next? [online]. [cit. 2024-02-29]. Dostupné z: https://online.maryville.edu/blog/evolution-social-media/
14. MĚŠEC.CZ. Vyznejte se v podvodech. Co je phishing, vishing, smishing a spoofing? [online]. [cit. 2024-02-29]. Dostupné z: https://www.mesec.cz/clanky/vyznejte-se-v-podvodech-co-je-phishing-vishing-smishing-ransomware-a-dalsi/
15. NEJPRIPOJENI. Z historie internetu [online]. [cit. 2024-02-29]. Dostupné z: https://nejpripojeni.cz/clanky/z-historie-internetu/
16. Příručka RESIST. In: Centrum proti hybridním hrozbám Ministerstva vnitra České republiky [online]. Praha: Ministerstvo vnitra České republiky, c2024 [cit. 2024-02-29]. Dostupné z: https://www.mvcr.cz/chh/soubor/resist-cz-pdf.aspx

17. Přispěvatelé Wikipedie, Dějiny internetu [online], Wikipedie: Otevřená encyklopedie, c2024, Datum poslední revize 9. 01. 2024, 09:33 UTC, [citováno 29. 02. 2024]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=D%C4%9Bjiny_internetu&oldid=23545849
18. Přispěvatelé Wikipedie, Globalizace [online], Wikipedie: Otevřená encyklopedie, c2024, Datum poslední revize 20. 02. 2024, 10:27 UTC, [citováno 29. 02. 2024] https://cs.wikipedia.org/w/index.php?title=Globalizace&oldid=23677425
19. Přispěvatelé Wikipedie, Kyberšikana [online], Wikipedie: Otevřená encyklopedie, c2024, Datum poslední revize 29. 01. 2024, 11:45 UTC, [citováno 29. 02. 2024]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Kyber%C5%A1ikana&oldid=23604206
20. Přispěvatelé Wikipedie, Sociální síť [online], Wikipedie: Otevřená encyklopedie, c2024, Datum poslední revize 25. 02. 2024, 18:37 UTC, [citováno 29. 02. 2024]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Soci%C3%A1ln%C3%AD_s%C3%AD%C5%A5&oldid=23691281
21. ŠANCE DĚTEM. Jak internet ovlivňuje život dětí a dospívajících? [online]. [cit. 2024-02-29]. Dostupné z: https://sancedetem.cz/jak-internet-ovlivnuje-zivot-deti-dospivajicich
22. TURBONET. Co je to internet a jak vlastně funguje? [online]. [cit. 2024-02-29]. Dostupné z: https://turbonet.cz/odpovedi-internetove-pripojeni/co-je-to-internet-a-jak-vlastne-funguje
23. WIKISOFIA. Sociální síť [online]. [cit. 2024-02-29]. Dostupné z: https://wikisofia.cz/wiki/Sociální_síť