POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

Katedra managementu a informatiky

Bezpečnost informací na sociálních sítích

Bakalářská práce

Information Security on Social Networks

Bachelor thesis

VEDOUCÍ PRÁCE

Ing. Bc. Hana DŮBRAVOVÁ

AUTOR PRÁCE

Natálie SNÁŠELOVÁ

PRAHA

2024

Čestné prohlášení

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

V Praze, dne 26. 2. 2024

……..

Snášelová Natálie

Poděkování

Ráda bych zde vyjádřila své upřímné poděkování Ing. Bc. Haně Důbravové za její cenné vedení a podporu při mé bakalářské práci. Její odborné rady, trpělivost a ochota vždy byly pro mě nepostradatelnými pomocníky během celého procesu výzkumu. Její zkušenosti a odbornost přispěly k tomu, že práce dosáhla svého účelu a cílů. Děkuji jí za inspiraci, motivaci a profesionální přístup k mému vzdělávání.

ANOTACE

Tato bakalářská práce se zaměřuje na problematiku bezpečnosti informací na sociálních sítích. Práce obsahuje stručný přehled nejznámějších sociálních sítí a jejich charakteristik. Dále se zabývá definicí hrozeb spojených se sdílením osobních údajů na těchto platformách a představuje preventivní programy a opatření k ochraně uživatelů před různými formami kybernetických hrozeb. Výsledky práce přinášejí ucelený pohled na problematiku bezpečnosti na sociálních sítích a mohou sloužit jako podklad pro tvorbu bezpečnostních politik a strategií v této oblasti.

KLÍČOVÁ SLOVA

*bezpečnost *sociální sítě *informace *data *prevence *hrozby *Edukace *osobní údaje *internet

ANNOTATION

This bachelor thesis focuses on the issue of information security on social networks. The work provides a brief overview of the most well-known social networks and their characteristics. Furthermore, it addresses the definition of threats associated with sharing personal data on these platforms and presents preventive programs and measures to protect users from various forms of cyber threats. The methodology of the thesis involves the analysis of available sources and studies dealing with security on social networks, as well as the comparison of different approaches to the prevention and resolution of these issues. The results of the work offer a comprehensive view of security issues on social networks and can serve as a basis for the development of security policies and strategies in this area.

KEYWORDS

*security *social networks *informations *data *prevention *threat *education *personal data *internet

Obsah

ÚVOD

V dnešní digitální éře, kdy sociální sítě prostupují téměř každou sférou našeho života a staly se nezbytnou součástí naší komunikace a interakce s okolním světem, se otázka bezpečnosti informací na těchto platformách stává nesmírně aktuální a důležitou. Sociální média se stala klíčovým prostředkem pro sdílení zkušeností, budování sociálních vazeb, komunikaci s ostatními a získávání informací o světě kolem nás. Nicméně s tímto rapidním rozvojem digitálního prostředí roste i riziko pro uživatele, a to v podobě zneužití osobních dat, kyberšikany, šíření dezinformací a dalších nebezpečí, která by neměla být podceňována.

Tato bakalářská práce, jež se zaměřuje na téma bezpečnosti informací na sociálních sítích, si klade za cíl poskytnout komplexní pohled na problematiku bezpečnosti v digitálním prostředí a přispět k prohloubení znalostí veřejnosti o rizicích a možnostech prevence. Hlavním cílem je detailně analyzovat povědomí uživatelů o různých typech hrozeb spojených s používáním sociálních sítí, a to od ztráty soukromí po možné finanční podvody. Dále se tato práce věnuje posouzení osobních zkušeností respondentů s různými formami rizik na sociálních sítích a jejich reakce na ně. Vedle toho se zaměřuje na hodnocení toho, zda si uživatelé dostatečně uvědomují důležitost ochrany svého soukromí a jakými opatřeními se snaží minimalizovat rizika spojená se sdílením informací online. Posledním klíčovým cílem práce je ověřit míru edukace uživatelů o bezpečnosti na sociálních sítích a zhodnotit úroveň informovanosti veřejnosti v této oblasti, přičemž se zaměřuje zejména na to, zda existuje potřeba posílení edukačních programů v této oblasti.

Pro dosažení stanovených cílů bude využita metoda řízeného strukturovaného rozhovoru, která poskytuje možnost podrobného zkoumání názorů, postojů a zkušeností respondentů týkajících se bezpečnosti informací na sociálních sítích. Tato metoda umožní získat hlubší porozumění tomu, jak uživatelé vnímají různá rizika a jakými způsoby se s nimi vyrovnávají. Respondenti budou osloveni s předem definovanými body, které pokrývají široké spektrum témat spojených s bezpečností na sociálních sítích, a jejich odpovědi budou podrobně analyzovány a interpretovány.

Očekávanými výstupy této bakalářské práce jsou doporučení, která mohou přispět k větší osvětě veřejnosti o bezpečnosti na sociálních sítích a k posílení ochrany osobních dat v digitálním prostředí. Tato práce má za cíl přispět k vytvoření

bezpečnějšího a informovanějšího digitálního prostředí pro všechny uživatele sociálních sítí.

Kromě toho lze očekávat, že výsledky této práce přinesou podrobnější pochopení současného stavu povědomí a postojů uživatelů k bezpečnosti na sociálních sítích. Díky detailní analýze zkušeností respondentů s různými formami rizik a opatření k ochraně soukromí bude možné identifikovat klíčové oblasti, ve kterých je zapotřebí zlepšení a další výzkum. V neposlední řadě lze předvídat, že výsledky této práce poslouží i jako podklad pro budoucí výzkumné projekty a studie zabývající se bezpečností na sociálních sítích a digitální bezpečností obecně. Důsledkem toho bude možné vytvořit nové strategie a iniciativy, jež se zaměří na posílení ochrany uživatelů v online prostředí a také na snížení rizik spojených s používáním sociálních sítí.

METODIKA VÝZKUMNÉHO ŠETŘENÍ

Ke zpracování praktické části bakalářské práce jsem si vybrala strukturovaný řízený rozhovor, který byl pojat kvalitativní metodou. Pomocí informací získaných studiem tohoto tématu jsem si stanovila body, podle nichž jsem rozhovor vedla. Při sestavování jednotlivých bodů jsem vycházela z teoretické části mé práce, která mi dala dostačující náhled do dané problematiky. Avšak věřím, že při případné verifikaci bych zvolila kvantitativní metodu, aby bylo možné dané výsledky porovnat se širší skupinou dotazovaných. Dle mého názoru je šetření formou strukturovaných rozhovorů nejvhodnější vzhledem k rozmanitosti daného tématu. Odpovědi dotazovaných mnohdy obsahovaly zajímavé subjektivní názory, které jsem dále rozepsala v empirické části. Respondentů jsem si vybrala deset na základě subjektivního zvážení a podobného věku. Byli genderově vyrovnaní a jejich věk se pohyboval od devatenácti do dvaceti čtyř let. Úvod rozhovoru měl za úkol zjistit základní informace o používání sociálních sítí konkrétním respondentem, kterými jsou například jaký čas tráví denně na sociálních sítích, od kolika let se pohybují v tomto prostředí nebo jaké sociální sítě používají nejčastěji. Toto mi dalo jasnou představu o tom, jak moc jsou dotazovaní na sociálních sítích aktivní. Další část rozhovoru byla strukturována do čtyř kategorií, kterými jsem zjišťovala jejich zkušenosti a povědomí o rizicích, opatřeních či edukaci. První bodem byla zkušenost dotazovaného ve vztahu k rizikům bezpečnosti informací na sociálních sítích. Na tuto část navazovala druhá, jež měla za úkol zjistit, jakých rizik na sociálních sítích si jsou účastníci rozhovoru vědomi. Po popsání osobních zkušeností a vydefinování rizik jsme se přesunuli ke třetí části, která měla za úkol zjistit opatření uživatelů před možným zneužitím informací a před dalšími riziky. Poslední část byla zaměřena na edukaci k tomto konkrétním odvětví, kdy respondenti mluvili o své formě současného vzdělávání. Tento přístup umožnil detailní a systematické zkoumání jednotlivých aspektů bezpečnosti na sociálních sítích. Data získaná prostřednictvím rozhovorů byla analyzována s cílem poskytnout užitečné poznatky a doporučení v oblasti ochrany osobních údajů na sociálních sítích.

TEORETICKÁ ČÁST

1 Vymezení pojmu kybernetické bezpečnosti a pojmů s tím souvisejících

V první kapitole této práce budou vymezeny pojmy kybernetické bezpečnosti a rovněž koncepty, které s ní úzce souvisí. Pojmy jako „bezpečnost“, „riziko“, nebo „kyberprostor“ jsou naprosto klíčové k pochopení této problematiky. Byť se s nimi poměrně často setkáváme, ne každý je dokáže nadefinovat nebo vysvětlit tak, aby vystihl jejich pravý význam. Vzhledem k podstatě a rozsahu práce nelze vydefinovat všechna pojmosloví, jež s touto problematikou souvisejí, proto se zaměřím hlavně na ta nejdůležitější, díky nimž bude možné pochopit danou problematiku rozebíranou v této práci.

1.1 Základní pojmy

Při přiblížení k samotnému konceptu kybernetické bezpečnosti je vhodné se zaměřit na analýzu tohoto termínu. Slovo „kyber“ zde odráží propojenost s prvky informačních a komunikačních technologií a také se samotným kyberprostorem. V něm se odehrává celá škála procesů včetně komunikace, zábavy, vzdělání nebo obchodu. Nabízí mnoho možností a směrů, kterými se lze vydat. Avšak tato kvanta výhod jsou spojena s obrovským rizikem v rámci kybernetické bezpečnosti, která se zabývá ochranou informací a dat před kybernetickými hrozbami a útoky, jako jsou například phishing, malware, útoky typu ransomware a mnohé další. V dnešní době je kyberprostor nezbytnou součástí našich každodenních činností a spolu s nárůstem hrozeb rovněž vzniká mnoho různých bezpečnostních opatření a prvků, které nám pomohou ochránit naše data a soukromí. To však neznamená, že si není třeba dávat pozor na to, co, kam či s kým sdílíme, nebo na co klikáme. Je důležité si stále uvědomovat všechna možná rizika, a přizpůsobit jim naše chování v kyberprostoru.

Bezpečnost

Bezpečnost je komplexní pojem, který zahrnuje širokou škálu aspektů od bezpečnosti fyzické, sociální, enviromentální, kybernetické, průmyslové až po cestovní. Každý druh bezpečnosti má svá specifika, jež jsou oproti ostatním druhům navíc. Avšak princip vždy vychází z definice bezpečnosti jako takové, kterou můžeme vymezit jakožto „stav, kdy jsou na nejnižší možnou míru limitovány hrozby pro objekt

(zpravidla národní stát, popř. i mezinárodní organizace) a jeho zájmy a tento objekt je k eliminaci stávajících i potenciálních hrozeb efektivně vybaven a ochoten při ní spolupracovat.“[1]

Kybernetická bezpečnost

Uživatelé nejen sociálních sítí má milnou představu o své bezpečnosti na internetu. Může za to ve většině případů nevědomost. Člověk má pocit, že stažením bezplatného antiviru se jeho počítač nebo jiné zařízení stává nedobytným. Toto je však velký omyl a řada lidí se neuvědomuje, že bezpečnostní hrozby mohou mít také jiný charakter než například malwarové útoky. Za spoustou nebezpečí může stát člověk, který vůbec necílí na údaje ve vašem počítači, ale sbírá informace, které uživatelé sami dávají veřejně na své sociální sítě. Samotnou kybernetickou bezpečnost bychom tedy mohli definovat jako „souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost.“[2]

Sociální sítě

Sociální sítě představují nezaměnitelný prvek moderního digitálního věku. Jsou to online platformy, které propojují uživatele, umožňují jim sdílet obsah, komunikovat a budovat virtuální komunity. V rámci pojmů virtuálního světa můžeme sociální sítě definovat 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.“[3] Lidé mohou prezentovat své životy, zájmy, pracovní činnosti či názory skrze textové příspěvky, fotografie, videa a další formy obsahu. To umožňuje interakci a propojení jednotlivců bez ohledu na jejich polohu.

---

[1] ZEMAN, Petr. *Česká bezpečnostní terminologie: Výklad základních pojmů*. Online. [cit. 2023-12-05]. Dostupné z: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048. Str. 13

[2] Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. [online]. [cit. 30. 11. 2023]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf s. 5.

[3] *Sociální sítě - INTERNETEM BEZPEČNĚ.* Online. [cit. 2023-12-05]. Dostupné z: view-source:https://www.internetembezpecne.cz/internetem-bezpecne/socialni-media/socialni-site/.

Informace a data

Ochrana osobních údajů se stala klíčovým tématem v souvislosti se sociálními sítěmi. Uživatelé často sdílejí citlivé informace o svém životě, a to může vyvolávat obavy ohledně soukromí a bezpečnosti. Je důležité si uvědomit, co vlastně jsou data a co informace, aby bylo možné porozumět tomu, jak je chránit. Informace „jsou údaje, které byly zpracovány do podoby užitečné pro příjemce. Každá informace je tedy údajem, datem, ale jakákoli uložená data se nemusejí nutně stát informací.“[4] Z toho vyplývá, že data jsou stavebním kamenem pro informace, a můžeme je tedy definovat jako „jakékoli prvky s informační hodnotou, které jsou zpracovávány počítačovým systémem, přičemž jsou zpracovávány tak, aby následně utvořily informaci.“

1.2 Související pojmy

A nyní je důležité probrat další pojmy.

Kyberprostor – Je „označení pro virtuální realitu interaktivního počítačového světa. Laicky řečeno je kyberprostor veškerý internet jako takový.“[5]

Riziko – Znamená „možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí. Riziko je vždy odvoditelné a odvozené z konkrétní hrozby. Míru rizika, tedy pravděpodobnost škodlivých následků vyplývajících z hrozby a ze zranitelnosti zájmu, je možno posoudit na základě tzv. analýzy rizik, která vychází i z posouzení naší připravenosti hrozbám čelit.“[6]

Kyberšikana – Je „druh šikany využívající informační a komunikační technologie (počítače, tablety, mobilní telefony, sociální sítě, emaily apod.) k ublížení druhému (vydírání, ubližování, ztrapňování, obtěžování, ohrožování, zastrašování apod.). Aktéry kyberšikany jsou (obdobně jako u klasické šikany): Agresor – Oběť – Přihlížející (publikum).“[7]

---

[4] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-34-8.Str.47

[5] *Co je to kyberprostor? - Správa.sítě.eu.* Online. 2022. [cit. 2023-12-05]. Dostupné z: view-source: https://www.sprava-site.eu/kyberprostor/.

[6] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Riziko - Ministerstvo vnitra České republiky*. Online. 2023, 2023. [cit. 2023-11-29]. Dostupné z: https://www.mvcr.cz/clanek/riziko.aspx

[7] *Kyberšikana - INTERNETEM BEZPEČNĚ.* Online. C2018. [cit. 2024-01-19]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/.

Hrozba – Hrozbou se myslí „jakýkoli fenomén, který má potenciální schopnost poškodit zájmy a hodnoty chráněné státem. Míra hrozby je dána velikostí možné škody a časovou vzdáleností (vyjádřenou obvykle pravděpodobností čili rizikem) možného uplatnění této hrozby.“[8]

Aktivum – Aktivem „se rozumí cokoliv, co má určitou hodnotu pro osobu, organizaci či stát. Aktivum může být věcí hmotnou (budova, počítačový systém, sítě, energie, zboží aj.) či nehmotnou (informace, znalosti, data, programy aj.) z pohledu občanského práva. Aktivem však může být i vlastnost (např. dostupnost a funkčnost systému a dat aj.) či dobré jméno, reputace atd. Lidé (uživatelé, administrátoři aj.) a jejich znalosti a zkušenosti jsou také z pohledu kybernetické bezpečnosti aktivem.“

Zranitelnost – Zranitelnost (vulnerability) „označuje slabé místo aktiva, softwaru, zabezpečení, které je využito jednou nebo více hrozbami. Zranitelnost, stejně jako hrozba, může být způsobena celou řadou faktorů spočívajících jak v jednání člověka, technické závadě, tak případně zásahu vyšší moci.“

Důvěrnost – Tento „pojem […] definuje tu skutečnost, že k informacím, datům, či ICT mají přístup pouze subjekty, které jsou k tomu autorizované (oprávněné).“

Kyberkriminalita – Je definována „jako jednání namířené proti počítačovému systému, počítačové síti, datům či uživatelům nebo jako jednání, při němž je počítačový systém použit jako nástroj pro spáchání trestného činu.“[9]

Kybernetická hrozba – Tyto „hrozby, nebo také hrozby kybernetické bezpečnosti jsou jakékoliv možné škodlivé útoky na data nebo IT vybavení organizace, jejichž cílem je neoprávněný přístup k datům, narušení IT systémů nebo poškození informací. Útoky mohou být nahodilé nebo mohou být cílené, organizované a mohou pocházet od jednotlivců, nebo od různých subjektů, včetně teroristických skupin, nepřátelských národních států, zločineckých organizací, hackerů ale mohou pocházet i zevnitř organizace od nespokojených zaměstnanců nebo firemních špiónů.“[10]

---

[8] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Hrozba*. [online]. [cit. 28. 11. 2023]. Dostupné z: http://www.mvcr.cz/clanek/hrozba.aspx

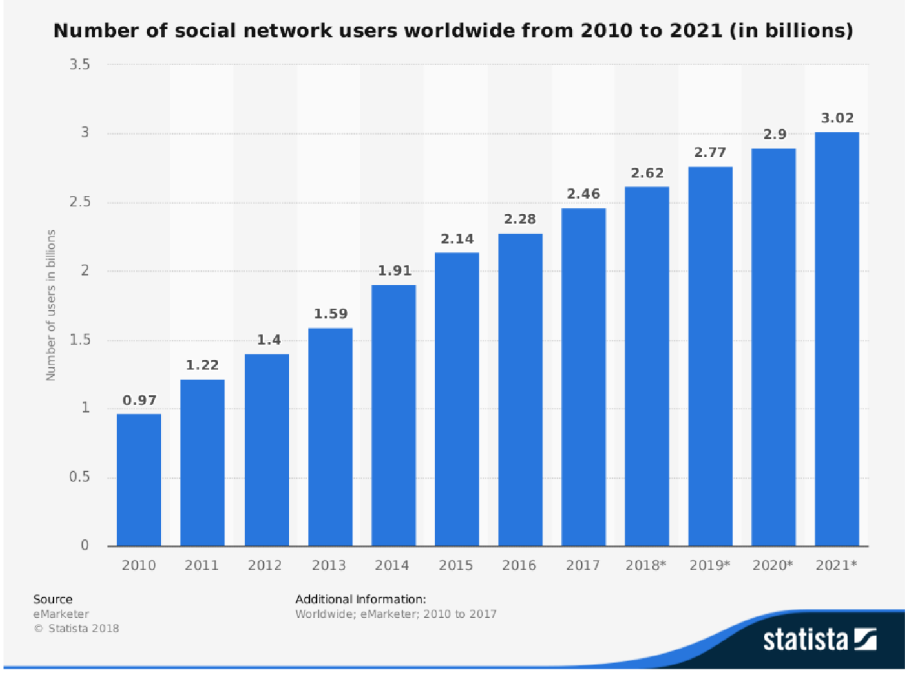
[9]KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-34-8.Str.48, 72, 89

[10] *Co jsou to kybernetické hrozby | Kybernetická bezpečnost | Aptien*. Online. 2023. [cit. 2023-12-05]. Dostupné z: view-source:https://aptien.com/cs/kb/articles/what-are-cybersecurity-threats.

2 Sociální sítě

Sociální sítě jsou důležitým prvkem moderní digitální éry, který dramaticky ovlivnil způsob, jakým lidé komunikují, sdílejí informace a budují své sociální vztahy. Tyto online platformy umožňují uživatelům propojit se s lidmi po celém světě. Zároveň vytvářejí prostor pro online komunitní interakce a dávají uživatelům možnost sledovat aktuality, získávat informace a zapojovat se do různých diskuzí. Od začátku 21. století, kdy začaly vznikat první sociální sítě, prošla tato média rapidním vývojem a stala se nedílnou součástí každodenního života miliard lidí po celém světě. Sociální síť tedy představuje online prostor, kde registrovaní uživatelé navzájem komunikují, sdílejí informace, fotografie, videa a mohou využívat další doplňující funkce. Přestože sociální sítě nabízejí mnoho přínosů a příležitostí, současně s sebou nesou i určitá rizika a výzvy. Patří sem otázky týkající se ochrany osobních údajů, kyberšikany, šíření dezinformací a negativního vlivu na duševní zdraví. S narůstajícím významem sociálních sítí ve společnosti je klíčové porozumět těmto aspektům a aktivně pracovat na vytváření bezpečného a zdravého online prostředí pro všechny uživatele.

První sociální sítě se objevily na přelomu tisíciletí, s platformami jako Six Degrees nebo Friendster. Následně přišly další významné sociální sítě, které ovlivnily masovou komunikaci. Facebook, založený Markem Zuckerberem v roce 2004, se stal jednou z nejpopulárnějších a nejrozšířenějších sociálních platforem na světě. Dalšími významnými sítěmi jsou pak v dnešních dnech X, LinkedIn, TikTok, Instagram a Snapchat. V současné době existují stovky různých sociálních sítí. Aktivně je využívají více než 3 miliardy lidí, což představuje polovinu světové populace. Níže lze vidět graf počtu uživatelů sociálních sítích zobrazených v rámci let 2010-2021.



Obrázek 1 - četnost uživatelů sociálních sítí v letech 2010-2021

Většina sociálních sítí pochází z USA a Číny, avšak najdeme i takové, jež jsou výhradně české. Ještě před několika lety lidé aktivně používali sociální sítě jako například Dikobraz.cz, Lide.cz, Bezones.cz, Libimseti.cz, Sousede.cz, Alik.cz a tak dále. Mnohé české sociální sítě se vytvářely prostřednictvím obsahových webových stránek, blogovacích portálů, diskuzních a recenzních fór a komunitních portálů. Příchod Facebooku na český trh způsobil výrazné změny ve vnímání sociálních sítí a mnoho komunitárních projektů začalo upadat. Uživatelé přešli na Facebook a v některých případech i na další mezinárodní platformy.[11] Mezi největší a nejznámější světové sociální sítě se v dnešní době stále řadí Facebook, který používá více než 3,03 miliardy uživatelů. Na druhém místě je YouTube s 2,5 miliardou uživatelů, třetí místo podle výzkumu z roku 2023 obsadil WhatsApp se 2 miliardami uživatelů a na čtvrté příčce je Instagram – taktéž se dvěma miliardami uživatelů.[12]

[11] *Sociální sítě: Přehled, seznam a žebříček největších a nejoblíbenějších*. Online. [cit. 2024-01-15]. Dostupné z: https://sitevhrsti.cz/socialni-site/.
[12] *23 Top Social Media Sites for Your Brand in 2024, Ranked*. Online. 2023. [cit. 2024-01-15]. Dostupné z: view-source: https://buffer.com/library/social-media-sites/.

2.1 Facebook

Jednou z nejznámějších sociálních sítí dnešní doby je Facebook. Facebook byl původně navržen, pro studenty Harvardské Univerzity, Markem Zuckerbergem, Eduardem Saverinem, Dustinem Moskovitzem a Chrisem Hughesem v roce 2004. Od roku 2006 už se k této sociální síti mohl zdarma připojit kdokoliv starší 13 let vlastnící e-mailovou adresu. Dnes je to největší síť na světě s téměř třemi miliardami uživatelů.[13]

Na Facebooku mohou uživatelé vytvářet své profily, sdílet fotografie, přidávat se k existujícím skupinám a zakládat nové skupiny. Platforma nabízí různé funkce, jako jsou časové osy, prostor na profilu každého uživatele pro zveřejňování obsahu a dostávání zpráv od přátel. Funkce jako „stav" umožňuje uživatelům sdílet svou aktuální polohu nebo situaci, zatímco News Feed poskytuje aktualizace o změnách v profilech a stavech „přátel". Uživatelé mohou také interagovat prostřednictvím chatu a posílat si soukromé zprávy. Celý tento koncept byl založen na transparentnosti uživatelů, jelikož jeden ze spoluzakladatelů, Mark Zukerberg, od samého začátku chtěl, aby se uživatelé prezentovali takoví, jací ve skutečnosti jsou.[14]

2.1.1 Bezpečnostní nedostatky

Facebook má stejně jako ostatní sociální sítě spoustu bezpečnostních nedostatků. Většina z nich se týká oblasti osobních informací, které uživatele sdílejí jak vědomě, tak nevědomě. Není výjimkou, že jsou tyto informace zneužívány, a ani Facebook se nevyhnul četným sporům kvůli neoprávněnému nakládání s daty. Některé bezpečnostní nedostatky mohou lidem značně znepříjemnit život. Jsou jimi například:

- Pokud uživatel rozhodne o zrušení svého profilu na Facebooku, veškeré informace, které na něj přidal, zůstanou nadále archivovány v databázi Facebooku. Stejně tak jeho příspěvky, fotografie a další obsah zůstávají na místech, kde byly původně sdíleny nebo jinak šířeny, například mezi ostatními uživateli. Toto pravidlo platí i v případě, že se uživatel rozhodne pouze odstranit konkrétní informaci nebo fotografii.
- Facebook automaticky analyzuje údaje, které uživatelé zveřejnili, jako jsou pohlaví, zájmy a věk, a sleduje jejich aktivity na účtu, včetně toho, které

[13] *Facebook: Getting Started with Facebook*. Online. [cit. 2024-01-16]. Dostupné z: view-source: https://edu.gcfglobal.org/en/facebook101/getting-started-with-facebook/1/.
[14] *Facebook | History, Features, Description, & Facts | Britannica*. Online. 2023. [cit. 2024-01-16]. Dostupné z: https://www.britannica.com/topic/Facebook.

reklamy otevřeli. Na základě těchto informací vytváří klíč, jenž určuje, jaké reklamy uživateli zobrazit. Současně jsou zaznamenávány veškeré aktivity uživatele na Facebooku.

- Facebook získává údaje z počítače, mobilního telefonu nebo jiného zařízení, které uživatel používá pro přístup k této sociální síti. Mezi tyto informace patří data o čase a místě, kde byly navštíveny stránky Facebooku, IP adresa, typ prohlížeče a operačního systému, který uživatel používá, a adresy stránek, jež prohlížel.
- Dokud uživatel sám nenastaví bezpečnostní opatření svého profilu, systém je automaticky nastaven tak, aby zveřejňoval co nejvíce informací.[15]

2.2 YouTube

YouTube je sociální platforma pro sdílení videí vyvinutá v roce 2005 Stevem Chenem, Chadem Hurleyem a Jawedem Karimem, která vznikla na myšlence sdílení svých domácích videí mezi větší skupinu lidí. Krátce po jejím spuštění se na sociální síti denně objevovalo kolem 30 000 návštěvníků. Čísla a popularita raketově rostla a v roce 2006 se tento počet zvýšil na více než 25 milionů zhlednutí. Denně bylo nahráváno více než 20 000 nových videí a o půl roku později to již bylo více než 100 milionů videí denně.

Tento velký nárust však způsoboval společnosti mnoho problémů. Museli nakupovat více počítačového vybavení a zlepšovat internetové připojení. Navíc s přibývajícími videi se zvedala i četnost soudních sporů zaměřených především na autorská práva. Později v roce 2006 se společnost Google koupila tuto síť s masivním počtem uživatelů za 65 miliard dolarů v akciích.[16]

2.3 WhatsApp

WhatsApp umožňuje rychlé posílání zpráv a bezplatné sdílení textových zpráv, videí, obrázků, gifů a dalších multimediálních souborů. Oproti běžným službám WhatsApp dovoluje posílat neomezené množství zpráv, což je jedním z klíčových faktorů, který přispěl k jeho rapidnímu vzestupu v popularitě v nedávných letech.

[15] LEPEŠKOVÁ, Bc. Lenka. *Facebook jako bezpečnostní hrozba*. Diplomová práce. Brno: Masarykova univerzita, 2011.
[16] *YouTube Britannica*. Online. 2023. [cit. 2024-01-17]. Dostupné z: https://www.britannica.com/topic/YouTube.

Aplikace se především používá na mobilních zařízeních, ale existuje i verze přístupná pro stolní počítače.

WhatsApp, aplikace pro rychlé zasílání zpráv, se vyznačuje funkcí, která ji výrazně odlišuje, a to neomezeným počtem znaků ve zprávách. Na rozdíl od běžných SMS, kde je člověk omezen počtem slov, lze přes WhatsApp posílat obsah bez jakýchkoli omezení. Další klíčovou výhodou WhatsAppu je, že neposkytuje jen potvrzení doručení, což je běžné u SMS, ale místo toho umožňuje sledovat aktuální stav vaší zprávy. To znamená, že je možné zjistit, zda byla zpráva přečtena, což přináší další úroveň komunikace.

Samotný název této platformy vznikl hravým spojením fráze „co se děje“ a slova „aplikace“. Od svého uvedení na trh v roce 2009 se WhatsApp stal nejoblíbenější aplikací pro zasílání zpráv na celém světě, shromažďující impozantní počet více než 1,5 miliardy aktivních uživatelů ve 180 zemích.[17]

WhatsApp, který náleží pod společnost Meta, avšak také sdílí osobní údaje uživatelů ostatním společnostem Mety. Jde především o telefonní číslo, údaje o transakcích, IP adresu, údaje o daném mobilním zařízení, nebo informace o službách a způsobech využívání této aplikace. Konverzace jsou chráněny šifrováním end-to-end a mají funkci soukromé konverzace, která by měla údajně zamezit Metě dostat se k informacím sdílených touto formou.[18]

2.4 Instagram

Instagram, platforma pro sdílení fotografií a videí, umožňuje sdílet příspěvky, které jsou umístěny na uživatelském profilu a mohou být prezentovány buď veřejně na Instagramu, nebo v režimu soukromí pro sledující uživatele. Uživatel má k dispozici dva hlavní kanály pro zveřejňování obsahu: trvalý profil, kde jsou příspěvky archivovány, a „Stories“ – speciální část, kde obsah zůstává dostupný po dobu 24 hodin, než automaticky zmizí, pokud není uložen. Uživatelé mají také možnost vysílat živě a streamovat videa přímo z kamery na tuto platformu. Vytvořit si zde účet může každý starší 13 let se svou e-mailovou adresou.

---

[17] *What is WhatsApp? Social Media Marketing Definitions - SocialBee*. Online. C2023. [cit. 2024-01-17]. Dostupné z: https://socialbee.com/glossary/whatsapp/.

[18] *Jaké informace WhatsApp se společnostmi Meta sdílí? | Centrum nápovědy pro WhatsApp*. Online. C2024. [cit. 2024-01-17]. Dostupné z: https://faq.whatsapp.com/1303762270462331/?locale=cs_CZ.

Sociální síť vznikla v roce 2010 díky spoluzakladatelům Kevinu Systromovi a Mikovi Kriegerovi. V současné době je součástí Meta Platforms (mateřské společnosti Facebooku). Instagram se vypracoval mezi přední světové sociální sítě a v roce 2022 zaznamenal významný milník – přesáhl dvě miliardy aktivních uživatelů měsíčně.

Tato sociální síť byla poprvé spuštěna pro veřejnost v App Store 6. října 2010 a hned po prvním dni dosáhla 25 000 uživatelů. Více než jeden milion uživatelů se zaregistrovalo do tří měsíců od zveřejnění, což byl naprosto fantastický úspěch. S rostoucí popularitou se začali objevovat také investoři a potencionální kupci. O necelé dva roky později byl Instagram prodán Meta Platforms za 1 miliardu dolarů v hotovosti a akciích Facebooku.[19]

2.5 TikTok

TikTok patří mezi nejrychleji rostoucí sociální sítě vůbec. Poprvé byl spuštěn v roce 2016 čínskou společností ByteDance, také známé jako Douyin. V roce 2017 se společnosti podařilo koupit konkurenční aplikaci Musica.ly, ze které převedla 200 milionů účtů na TikTok. K dnešnímu dni uživatelé čítají něco okolo dvou a půl miliard. Společnost ByteDance se tak mohla pyšnit nejhodnotnějším startupem na světě, jelikož samotný TikTok měl už v polovině roku 2020 údajnou hodnotu 50 miliard dolarů.

Samotná aplikace slouží ke sledovaní, tvoření a sdílení krátkých videí, k vytváření krátkých videoklipů, nebo například k živému vysílání. Nejvíce se proslavila trendem synchronizovaných sestav a tanečků, neboli Lip Sync, což jsou videa, kde je nutno sladit pohyby rtů s hudbou.

TikTok i přes zatím poměrně krátkou dobu působení čelil spousta obviněním z důvodu shromažďování dat nebo ze zveřejňování pornografie. Například v Indii byl zakázán už v roce 2020 a označen jako nebezpečí pro národní suverenitu. V únoru 2019 musela společnost zaplatit 5,7 milionů dolarů kvůli obvinění, že nezákonně shromažďovala osobní údaje od dětí.[20]

---

[19] *Instagram | History, Features, Description, & Facts | Britannica*. Online. 2023. [cit. 2024-01-16]. Dostupné z: https://www.britannica.com/topic/Instagram.

[20] *TikTok: What It Is, How It Works, and Why It's Popular*. Online. 2023. [cit. 2024-01-16]. Dostupné z: https://www.investopedia.com/what-is-tiktok-4588933.

Samotné používání TikToku přináší pro jeho uživatele značnou řadu rizik. Aplikace shromažďuje rozsáhlé množství dat o svých uživatelích, včetně velmi citlivých údajů, které nejsou přímo nezbytné pro její běžný chod. Kromě toho je třeba vzít v úvahu čínské právní prostředí, jež nařizuje čínským společnostem, a tedy i provozovatelům aplikací jako je TikTok, spolupracovat s vládou a poskytovat informace, aniž by byly poskytnuty odpovídající právní záruky.

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) v minulém roce dokonce vydal varování o tom, že takto aplikace představuje skutečnou bezpečnostní hrozbu. Výrazně jej nedoporučuje stahovat na zařízeních, které mají přístup k informačním a komunikačním systémům kritické informační infrastruktury, informačním systémům základní služby, nebo významným informačním systémům. Dále doporučuje, aby se stahování a používání vyvarovaly také osoby s vyšším společenským nebo vlivným postavením. V případě, že se uživatelé rozhodnou pokračovat v používání aplikace TikTok, budou nadále podrobeni rozsáhlému sběru dat, která nejsou nezbytná pro samotné fungování aplikace, ale mohou být potenciálně zneužita v budoucnosti. Ovšem samotné rozhodnutí o dalším používání zůstává na každém jednotlivci.[21]

2.6 X

Sociální síť X, známá spíše pod svým starým jménem Twitter, je platformou, na níž byli původně zveřejňovány krátké články o maximální délce 280 znaků. Byla založena v roce 2004 Evanem Williamsem, Bizem Stonem a Noahem Glassem a původně sloužila k publikování podcastů. V roce 2005 však Apple oznámil, že do iTunes přidá své podcasty také, a zakladatelé se proto shodli, že kvůli konkurenci změní zaměření své aplikace. Byli tázáni, zda se nechtějí zaměřit spíše na mini blogy, na kterých by si přátelé mohli sdílet své životy. Noah Glass tedy navrhl jméno „Twitter“ a zprávy pojmenovali Tweety. Nová verze byla spuštěna v roce 2006. V roce 2015 přidali novou funkci s názvem „momenty“, kterou v roce 2017 nahradila funkce Prozkoumat. Zde si lidé mohou ukládat tematické sbírky tweetů a dalšího obsahu. O rok později byla nahrazena chronologická časová osa tweetů za algoritmickou. To

[21] Národní úřad pro kybernetickou a informační bezpečnost - Aplikace TikTok představuje bezpečnostní hrozbu. Online. 2023. [cit. 2024-01-16]. Dostupné z: https://nukib.gov.cz/cs/infoservis/hrozby/1941-aplikace-tiktok-predstavuje-bezpecnostni-hrozbu/?fbclid=IwAR22tQZQXC6EyXEuPCIAQPzZRgm7en7LaHQNhpdtDNmN3nHfdTK1_TaHRQ8.

znamená, že se na hlavní stránce neukazují tweety podle času, ale podle oblíbenosti mezi ostatními uživateli a mezi uživateli, které daný člověk sleduje. V roce 2022 koupil Twitter Elon Musk za 44 miliard dolarů a o rok později jej oficiálně přejmenoval na „X“.[22]

2.7 Bezpečnostní opatření na sociálních sítích

Kybernetickým útokům, které mají za cíl shromažďovat osobní informace za účelem možného zneužití, se lze bránit mnoha způsoby. Bohužel se občas stane, že přes veškerou opatrnost mohou uživatelská data uniknout, ať už kvůli nepozornosti, nebo zkušenému jednání opačné strany. Když pomineme nebezpečí ukládání uživatelských informací neoprávněnými stranami, stále je zde riziko zneužití samotnou sociální sítí. Tomuto riziku se nelze bránit jinak, než že samotou sociální síť nebude člověk používat. Bohužel v dnešní době jsou na sociální sítě často vázány i různé pracovní záležitosti a občas se bez účtu na síti člověk jednoduše neobejde.

Když už tedy sociální sítě používáme dobrovolně, nebo kupříkladu kvůli svému zaměstnavateli, je dobré dodržovat pár následujících bodů.

- Silná hesla jsou klíčová. Čím jsou delší, tím jsou bezpečnější. Je taky dobré používat kombinaci znaků, čísel, malých a velkých písmen.
- Různá hesla pro různé sociální sítě.
- Nastavte bezpečnostní otázky pro autentizaci.
- Zajistěte ochranu svého mobilního zařízení, pokud máte sociální sítě na telefonu.
- Buďte obezřetní při přijímání žádostí o přátelství. Nepřijímejte žádosti od lidí, které neznáte.
- Dávejte pozor na to, na co klikáte. I když obsah sdílí váš přítel, kdokoliv může zneužít jeho účet.
- Udržujte soukromí a vyvarujte se sdílení citlivých informací.
- Seznamte se s pravidly ochrany osobních údajů na svých sociálních sítích.
- Instalujte antivirový program a ujistěte se, že máte nejnovější aktualizace.
- Vždy se odhlašujte, abyste zabránili neoprávněnému přístupu.[23]

---

[22] *X | Company, History, Twitter, Elon Musk, & Uses | Britannica*. Online. 2024. [cit. 2024-01-24]. Dostupné z: https://www.britannica.com/topic/Twitter.

[23] *10 pravidel pro bezpečné surfování na sociálních sítích – KYBEZ. Online. 2020*. [cit. 2024-01-17]. Dostupné z: https://kybez.cz/10-pravidel-pro-bezpecne-surfovani-na-socialnich-sitich/.

3 Identifikace hrozeb

S nástupem sociálních sítí se rapidně zvedl i počet hrozeb, které mohou mít za následek mnoho nepříjemných komplikací. Někteří lidé v relativně novém online světě našli mnoho způsobů, jak jednoduše se lze obohatit, a to i za cenu, že to jde na úkor někoho druhého. Těchto nešvarů se pak dopouštějí také lidé, kteří by takové jednaní v osobním životě nikdy nepřipustili. Spousta podobných útoků jsou pak mířeny především na krádeže dat nebo poškození druhé osoby. Identifikace hrozeb na sociálních sítích je nezbytným prvkem k zajištění kybernetické bezpečnosti, neboť uživatelé těchto platforem jsou vystaveni různorodým rizikům spojených s digitálním prostředím.

Jednou z klíčových hrozeb je kyberšikana, která může zahrnovat různé formy obtěžování, od urážek po vydírání a také šíření falešných informací. Dalším rizikovým faktorem je vytváření falešných profilů a zneužívání identity. Uživatelé mohou být vystaveni riziku, kdy dojde k vytvoření falešných účtů s cílem klamání nebo poškození pověsti jiných. Zneužívání osobních údajů a jejich šíření bez souhlasu je též častým problémem. Kybernetická bezpečnost na sociálních sítích se musí vypořádat i s hrozbami jako je phishing a malware. Nepřátelské akce a hate speech jsou rovněž problematickými jevy. Sociální sítě mohou být prostředím pro šíření nenávisti, rasismu a nepřátelských postojů, což může vyvolat konflikty a ohrozit bezpečnost uživatelů. Další z hrozeb může být například kyberstalking neboli nežádoucí sledování a obtěžování jednotlivců online, což představuje další hrozbu. Toto chování zahrnuje i nedovolené sbírání informací o soukromém životě uživatelů. Identifikace těchto hrozeb vyžaduje komplexní přístup, který zahrnuje technologická opatření, vzdělávání uživatelů a aktivní sledování jejich chování na sociálních sítích. Je třeba, aby kybernetická bezpečnost na sociálních sítích efektivně kombinovala prevenci, detekci a reakci na tyto různorodé hrozby s cílem poskytnout uživatelům bezpečné online prostředí.

3.1 Zneužití osobních údajů

Rizikové mohou být i údaje, kterými se každý na sociálních sítích prezentuje, jako například jméno, příjmení nebo profilová fotografie. I takto obecné údaje mohou být zneužity kupříkladu tak, že si jiná osoba založí účet pod cizím jménem a cizí fotografií

a vydává se za někoho jiného. Toto může vést k mnoha nepříjemnostem, které mohou vyústit i v šikanu jak v kyberprostoru, tak ve fyzické a osobní rovině.

Osobní údaje zahrnují všechny informace, které souvisejí s konkrétní identifikovanou nebo identifikovatelnou osobou. Mezi ně patří i jednotlivé informace, které ve spojení mohou vést k identifikaci dané osoby. Typicky se mezi ně řadí kromě výše zmíněných také domácí adresa, e-mailová adresa, číslo občanského průkazu, lokační údaje, IP adresa nebo například telefonní číslo.[24]

Přesnou definici upravuje Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále GDPR), které uvádí, že „osobními údaji jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen ‚subjekt údajů'); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby."

3.1.1 Únik dat v roce 2018

Jeden z nejznámějších incidentů spojený se zneužitím dat se stal v roce 2018, kdy se do popředí dostala britská politická poradenská společnost. V březnu se deník The New York Times, dostal k dokumentům od firmy Cambridge Analytica, kterou vlastnil Robert Mercer. Tyto dokumenty odhalily, že firma, v níž byl zapojen i bývalý poradce Donalda Trumpa Stephen K. Bannon, neoprávněně využívala data z Facebooku k vytváření profilu voličů.

Zpravodajské kanály odhalily, že tato firma získala a následně využila osobní údaje uživatelů Facebooku původně shromážděné pro akademický výzkum. Původní odhad naznačoval, že Cambridge Analytica získala data od více než 50 milionů uživatelů Facebooku. Nicméně, technologický ředitel Facebooku Mike Schroepfer ve svém nedávném oznámení o nových funkcích ochrany soukromí představil aktualizovaný odhad, který se týkal až 87 milionů uživatelů, přičemž většina z nich byla z USA. Mnozí z nich přitom neposkytli společnosti žádný souhlas k použití svých dat

[24] *Co jsou to osobní údaje? - Evropská komise*. Online. [cit. 2024-01-17]. Dostupné z: https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_cs.

nebo nebyli informováni o tom, že jsou jejich údaje využívány. Tento skandál vedl k bankrotu Cambridge Analytica, zatímco Facebook čelil pokutě ve výši 5 miliard dolarů, kterou mu uložila Federální obchodní komise.[25]

3.1.2 Citlivé osobní údaje

Podle článku 9 odstavce 1 GDPR se citlivé údaje definují jako „osobních údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby“.

Tyto údaje lze zpracovat jen za určitých podmínek, kterými jsou například:

- „subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů, s výjimkou případů, kdy právo Unie nebo Členského státu stanoví, že zákaz uvedený v odstavci 1 nemůže být subjektem údajů zrušen;
- zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany, pokud je povoleno právem Unie nebo Členského státu nebo kolektivní dohodou podle práva Členského státu, v němž se stanoví vhodné záruky týkající se základních práv a zájmů subjektu údajů;
- zpracování je nutné pro ochranu Životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas;
- zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů;
- zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo pokud soudy jednají v rámci svých soudních pravomocí.“[26]

[25] CONFESSORE, Nicholas. *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far - The New York Times*. Online. The New York Times. 2018, roč. 2018. [cit. 2024-02-12]. Dostupné z: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

[26] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: 2016. [cit. 2024-02-12].

3.2 Krádež dat

Neoprávněné získávání digitálních dat od subjektu, obvykle s motivací finančního zisku nebo narušení obchodních aktivit, se nazývá krádež dat. Zahrnuje nezákonný přístup, přenos nebo ukládání citlivých údajů – od osobních a finančních informací po proprietární technologie, algoritmy a procesy.

Tato forma kybernetického útoku představuje závažné ohrožení bezpečnosti a soukromí s možnými ničivými následky. Ty mohou zahrnovat rozsáhlé sankce za nedodržení předpisů, poškozenou pověst a finanční a provozní ztráty. Krádeže dat mohou být iniciovány různými subjekty, včetně externích útočníků, správců systémů, zaměstnanců nebo jiných osob s nekalými úmysly, kteří získávají podniková data ze zabezpečených serverů, cloudových aplikací, databází nebo osobních zařízení.

Tyto data se mohou k útočníkovi dostat dvěma způsoby. První z nich bývá spojen s nekalými úmysly nebo aktivitami, včetně hackování, používání malwaru či zneužívání bezpečnostních chyb v systémech. Motivace za těmito úniky může být různorodá, sahající od touhy po finančním zisku, jak lze pozorovat v případech krádeží informací o platebních kartách, až po strategické výhody, jako jsou ukradená obchodní tajemství nebo vládní zpravodajské informace. Charakterizuje jej nepovolený přístup k zabezpečeným nebo důvěrným informacím, často prováděný neoprávněnými osobami.

Typickým znakem druhého ze způsobů je neúmyslné zveřejnění nebo odhalení osobních dat veřejnosti nebo jednotlivcům, kteří by k nim neměli mít přístup. Tato situace může být způsobena lidskou chybou, špatnou konfigurací nebo dokonce nedbalostí, jako například omylem zveřejněné citlivé informace na veřejném webu nebo jejím odeslání nesprávnému příjemci v e-mailu. I když v tomto případě nemusí existovat záměrný akt či přímé proniknutí, následky úniků mohou být stejně závažné, a vést tak například k poškození pověsti, finančním ztrátám nebo dokonce právním důsledkům.

3.2.1 Druhy krádeže dat

Krádeže dat na sociálních sítích mohou nastat z různých důvodů, zejména v důsledku technologických zranitelností, lidských chyb nebo záměrného zneužití. Níže je uveden přehled některých nejčastějších scénářů, při nichž může dojít ke krádeži dat na sociálních sítích:

- **Drive-by Stahování**: Návštěva kompromitovaného webu nebo sítě může automaticky stáhnout škodlivý software bez vědomí uživatele.
- **Nezabezpečené sítě**: Používání nešifrovaných nebo nedostatečně zabezpečených sítí, zejména veřejných Wi-Fi, může člověk vystavit data odposlouchávačům.
- **Sociální inženýrství**: Taktiky manipulace jednotlivců, které slouží k získání důvěrných informací nebo k ohrožení bezpečnosti dat.
- **Man-in-the-middle (MitM):** Útočníci skrytě odposlouchávají a v případě potřeby modifikují komunikaci mezi dvěma stranami s cílem odcizit data.
- **Falešné profily a podvody:** Identifikace falešných nebo podvodných profilů, které mohou být vytvořeny k účelu sběru informací nebo šíření škodlivých obsahů.
- **Phishingové útoky**: Kyberzločinci vytvářejí podvodné e-maily a zprávy, které vypadají jako legitimní. Cílem je přelstít příjemce a získat citlivé informace, například přihlašovací údaje nebo čísla kreditních karet. Níže je vyobrazen příklad podvodného e-mailu, kterým se útočník snaží získat přihlašovací údaje na Facebook od jiné osoby.

Obrázek 2 – ukázka podvodného e-mailu

3.2.2 Důsledky krádeže dat

Krádež dat není v žádném případě příjemná a může člověku hodně ublížit. Jedním z nejčastějších typů zneužívání osobních údajů získaných z dat je vytvoření identity jiné osoby. Zloději se snaží využít všech vašich osobních údajů, které se jim povedlo nashromáždit, a vytvoří si profil či účet na vaše jméno, jehož prostřednictvím

páchají škody. To může mít za důsledek pošpinění vašeho profesního nebo osobního jména, popřípadě také pošpinění vaší pověsti. V některých případech se může jednat například o rozesílání intimních fotografií, detailů nebo citlivých informací. Další velmi nepříjemný, a přesto velice častý důsledek je ztráta financí. Jedná se kupříkladu o neoprávněné výběry, nebo převody peněz prostřednictvím údajů, které se zlodějům podařilo získat.[27]

3.3 Kyberšikana

V dnešní době, kdy digitální komunikace tvoří nedílnou součást našeho každodenního života, se otevírá nový prostor pro sociální interakce, ale bohužel také pro nežádoucí jevy. Jedním z těchto negativních fenoménů je kyberšikana, obtěžování a šikanování prostřednictvím elektronických komunikačních kanálů. Téma kyberšikany se stává stále důležitějším, neboť se společnost stále více digitalizuje a lidé jsou propojeni pomocí internetu a sociálních médií. Samotnou kyberšikanu lze definovat jako „jakékoliv chování, jehož záměrem je vyvést z rovnováhy, ublížit, zastrašit nebo jinak ohrozit oběť za pomoci moderních informačních technologií.“[28]

V digitálním prostředí je kyberšikana považována za vážný problém, kde se jednotlivci stávají obětí různých forem obtěžování, zastrašování a ponižování online. Tato forma šikany může nabývat různých podob, ale vždy má za cíl poškodit oběť jak emocionálně, tak sociálně. Hlavní rysy kyberšikany zahrnují verbální útoky, sociální vyloučení, shaming a ponižování nebo vytváření falešných účtů a falešných identit.

Verbální útoky v podobě vulgarit, urážek a sarkastických komentářů jsou v prostředí kyberšikany běžné, jelikož anonymita online světa umožňuje agresorům vytvářet negativní atmosféru velice jednoduše. Sociální vyloučení může následovat, když jsou oběti záměrně izolovány nebo vynechány z online skupin a konverzací. Vytváření falešných účtů a identity slouží útočníkům k manipulaci s pověstí oběti, zatímco kyberstalkování zahrnuje sledování online aktivity oběti, což může být nepříjemné a invazivní. Fyzické a psychické důsledky kyberšikany jsou vážné a mohou zahrnovat úzkosti, deprese, sníženou sebedůvěru a v extrémních případech i sebevražedné myšlenky. Kyberšikana není omezena na konkrétní věkovou skupinu

[27] *What Is Data Theft? Definition, Examples & More | Proofpoint US*. Online. [cit. 2024-01-19]. Dostupné z: https://www.proofpoint.com/us/threat-reference/data-theft.
[28] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

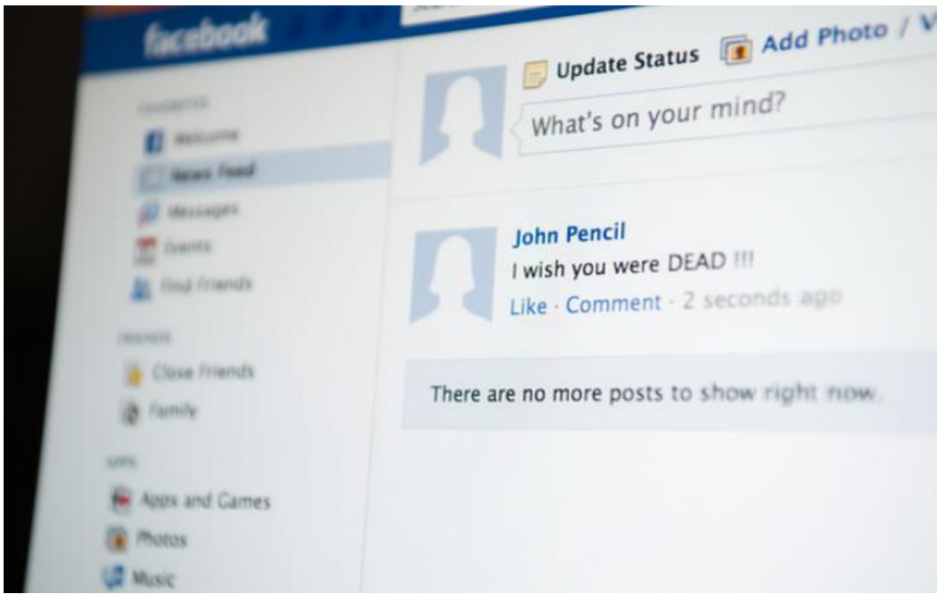
nebo sociální vrstvu; naopak, její dopady mohou postihnout jedince napříč různými demografickými skupinami.

3.3.1 Druhy kyberšikany

V dnešní společnosti je kyberšikana rozsáhlým fenoménem, který má negativní dopad na životy mnoha lidí. Každý druh představuje určitou hrozbu, jež má za cíl poškodit jinou osobu nebo osoby. Tyto druhy lze rozdělit následovně:

- **Sociální vyloučení**: Sociální vyloučení představuje záměrné ignorování jednotlivce. Například dítě může být evidentně vynecháno ze skupiny nebo akce, kterou ostatní diskutují nebo do níž jsou zapojeni. Taktéž může být opomenuto v rámci sdílených konverzací nebo zpráv, které zahrnují společné přátele.
- **Doxing:** Doxing představuje akci, při níž jsou bez souhlasu jednotlivce zveřejněny citlivé nebo osobní informace s úmyslem způsobit mu újmu nebo ho ponižovat. V rámci kyberšikany může doxing zahrnovat odhalení citlivých fotografií osoby bez jejího souhlasu nebo veřejné sdílení soukromých zpráv jednotlivce, například v online chatovací skupině.
- **Podvod:** V těchto případech se tyran se svým cílem spřátelí a uvede ho do klamného pocitu bezpečí. Až násilník získá důvěru svého cíle, zneužije této důvěry a zveřejní osobní informace oběti jiným lidem za účelem oběť poškodit.
- **Kybernetický stalking:** Jedná se o jednu z nejzávažnějších forem kyberšikany, jelikož má za cíl vyvolat v oběti strach o svou bezpečnost. Jedná se o jakékoliv sledování osoby v kyberprostoru, její kontaktování a tak podobně. Oběti jsou nuceny rušit si účty, nebo blokovat nově příchozí či ty stávající profily uživatelů. Agresor stále vymýšlí nové způsoby, jak oběť sledovat nebo kontaktovat prostřednictvím SMS, zpráv na sociálních sítích nebo e-mailem.
- **Fraping:** Tento pojem vznik ze dvou slov a to slova „Facebook“ a „Rape“, což znamená znásilnění. Jedná se o neoprávněné vniknutí na účet jiné osoby a zveřejňování obsahu za účelem dotyčnou osobu ponížit nebo ztrapnit. I když může být fraping považován za neškodný vtip ve chvíli, kdy je prováděn na přátelském základě, například při nechávání otevřeného telefonu nebo počítače, jeho zlomyslné provedení může mít závažné důsledky. Pro oběť může být fraping obzvláště problematický, pokud ohrožuje její identitu nebo poškozuje osobní pověst.

- **Masquerading:** Jedná se o založení online identity nebo profilu na osobu, která k tomu nedala oprávnění. Tato metoda často zahrnuje vytvoření fiktivní e-mailové adresy a stažení údajů z originálního účtu za účelem vydávat se za danou osobu. Tato metoda má poškodit osobu formou sdílení nebo rozesílání podvodného, škodlivého či jinak ponižujícího obsahu.
- **Dissing:** Je označení pro to, kdy tyranská osoba rozšiřuje nepravdivé či ponižující informace o své oběti prostřednictvím veřejných příspěvků nebo soukromých zpráv s cílem poškodit její pověst nebo vztahy s ostatními. V těchto situacích se tyranská osoba často snaží s poškozenou osobou udržovat vztah na kamarádské úrovni.
- **Trolling:** Trollující útočníci se záměrně snaží vyvolat negativní reakce tím, že publikují pobuřující nebo útočné komentáře online v rámci sociální skupiny. Mají tendenci zaměřovat se na vytváření konfliktů a obvykle nemají se svými oběťmi osobní vztah. Níže je vyobrazen příklad negativního příspěvku v rámci komunity.



Obrázek 3 – ukázka Trollingu

- **Flaming:** Jedná se o osobnější a přímější útok na jednotlivce, který obvykle probíhá v sociálním prostředí, jako jsou skupiny na sociálních sítích nebo

chatovací fóra. Pro flaming je typické používání vulgárních výrazů a urážlivých komentářů s cílem zastrašit oběť.[29]

3.3.2 Prevence kyberšikany

V dnešní digitální éře, kdy je společnost stále více propojená prostřednictvím internetu a sociálních médií, se otázky kybernetické bezpečnosti a prevence kyberšikany stávají neodmyslitelnou součástí našich životů. Je skoro až nemožné chránit se proti všem rizikům, které na nás číhají skrze sociální sítě. Můžeme se však snažit počet těchto rizik snižovat.

Prevenci lze rovněž chápat jako soubor intervencí, které mají za úkol snížit nebo úplně zabránit vzniku a rozšíření daného problému. Vyžaduje komplexní opatření, včetně právní ochrany, vytváření bezpečných online prostředí, vzdělávání o kybernetické etice a aktivního zapojení komunity do prevence a řešení těchto situací. Je nezbytné přijímat koordinovaný přístup, aby se ochránila bezpečnost a pohoda uživatelů digitálního prostředí

Prvním a základní krokem, na který by měl dbát každý uživatel sociálních sítí a internetu, je **Ochrana účtů a zařízení.** Je důležité mít na všech svých účtech a zařízeních hesla, která znáte jenom vy. Hesla by měla být složená z malých a velkých písmen, čísel a popřípadě i ze znaků. Nedoporučuje se si jako heslo nastavovat vlastní jméno nebo příjmení, neboť toto jsou nejčastější hesla všech uživatelů. Ochranou zařízení se také myslí nenechávat nikde vaše odložené zařízení, do kterého by se mohli dostat například jen kamarádi, neboť toto vytváří podmínky například pro fraping.

Většina sociálních sítí má v nastavení **prvky ochrany soukromí,** které vám pomůžou chránit se před agresorem přímo prostřednictvím funkcí dané používané sociální sítě. Nejspolehlivějšími prvky jsou nastavení účtu jakožto soukromého, vypnutí funkce označování vašeho profilu jinými lidmi, vypnutí komentářů, vypnutí sdílení vašich fotografií nebo nepřijímání příchozích zpráv od lidí, které nemáte v kontaktech nebo kterým jste nedali povolení váš účet sledovat.

[29] *The 10 Types of Cyberbullying - Blog*. Online. 2023. [cit. 2024-01-23]. Dostupné z: https://blog.securly.com/10/04/2023/the-10-types-of-cyberbullying/.

Udržujte osobní věci v soukromí, nesdílejte svou adresu, telefonní číslo nebo e-mailovou adresu. Je důležité si uvědomit, že i přes nastavení soukromého účtu mohou být mezi vašimi „známými“ lidé, kteří se za dotyčného člověka pouze vydávají.

Většina smartphonů v dnešní době umožňuje **sledování polohy.** Vaše časová osa navštívených míst se zaznamenává v telefonu a pokud máte povolené sdílení, mohou k ní mít přístup taky vaši známí. Skoro každá sociální síť má v podmínkách pro registraci a používání, že přístup k těmto údajům musí být povolen. Je dobré si tuto funkci vypnout všude, kde to jde, a u těch aplikací, u nichž není poloha potřeba ke správnému chodu.

Často se stává, že se neoprávnění lidé dostanou na váš účet kvůli tomu, že se někde zapomenete odhlásit. Nezapomeňte se proto **odhlašovat z veřejných zařízení.** Vniknutí cizí osoby na účet má za následek mnoho špatného. Nejenže může osoba zneužít vaše údaje ke kterým se lehce dostane, také vám může změnit nastavení soukromí nebo přes vaše jméno zveřejňovat nevhodný obsah. Myslete na to, že pouhé zavření karty mnohdy nestačí, a je potřeba se soustředit na odhlášení a odstranění účtu z paměti počítače.

Posledním a nejdůležitějším krokem je **nahlásit kyberšikanu**. Nahlásit ji můžeme hned několika způsoby. Zde však záleží, kdo kyberšikanu provádí (v mnoha případech to může být někdo, jehož totožnost je neznámá), kdo je oběť, zda kyberšikana probíhá například na pracovišti nebo ve škole, nebo jak moc závažná a nebezpečná je. Existují případy, kdy může být ohrožen život a fyzické nebo duševní zdraví osoby, a tyto případy řeší policie, proto je vhodné obrátit se na ni. Ty méně závažné případy, kterými jsou například zveřejňování příspěvků skrz kamarádův účet na základní škole, se dají řešit prostřednictvím školního psychologa a třídního pedagoga, tedy není nutné obracet se rovnou na policii. Nahlášení by však mělo probíhat i v kyberprostoru, a to prostřednictvím té sociální sítě, na níž k kyberšikaně došlo. Správci sítě prověří vaše nahlášení a účet či příspěvek mohou zablokovat, pokud se prokáže, že vaše nahlášení bylo právoplatné. To však nemusí být tak účinné řešení, jelikož si agresor může kdykoliv založit účet nový. Ve všech případech je to však doporučováno.[30]

[30] *How to Prevent Cyberbullying.* Online. 2022. [cit. 2024-01-24]. Dostupné z: https://www.verywellfamily.com/how-to-prevent-cyberbullying-5113808.

4 Preventivní programy

V dnešní době, kdy jsou sociální sítě klíčovým prvkem každodenního života, vzniká naléhavá potřeba zajistit bezpečí uživatelů v digitálním prostředí. S narůstajícím výskytem kybernetických hrozeb, zejména na sociálních médiích, nabývají preventivní programy bezpečnosti na těchto platformách zásadního významu. Česká republika má mnoho neziskových organizací, které se zabývají zvyšováním povědomí a prevencí hrozeb na internetu.

4.1 E-bezpečí

Certifikovaná iniciativa s celonárodním dosahem, projekt E-Bezpečí, je specializována na široké spektrum aktivit v oblasti prevence, vzdělávání, výzkumu, intervencí a osvěty v souvislosti s rizikovým chováním na internetu a přidruženými jevy. V poslední době se projekt rozšířil i do oblasti pozitivního využívání informačních technologií ve vzdělávání a každodenním životě. Za realizaci tohoto významného projektu stojí Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého, spolupracující s dalšími organizacemi. Zaměřuje se především na sexting, kyberšikanu, kyberstalking, stalking, online závislosti nebo zneužití osobních údajů v kyberprostředí.

Vychází ze systematické práce s různými cílovými skupinami, pořádání přednášek, a realizace preventivních vzdělávacích akcí a podobných aktivit. Při přednáškách a besedách se detailně analyzují konkrétní rizikové jevy, zároveň jsou představovány možnosti prevence a obrany proti potenciálním hrozbám. K porozumění problematiky přispívají jak modelové situace, tak reálné případy. Besedy jsou interaktivní, doplněné multimediálními prvky a obsahují prezentace a ukázky ve formě videí. Iniciativa se rovněž věnuje průběžným celorepublikovým výzkumným šetřením, která se zaměřují na analýzu rizikové komunikace v online prostředí. Současně poskytuje online poradenství, vytváří informační materiály pro žáky a učitele a aktivně se podílí na šíření povědomí o bezpečném chování na internetu. Široké spektrum aktivit projektu zahrnuje další iniciativy směřující k osvětě a prevenci v oblasti kybernetické bezpečnosti.[31]

[31] *Informace o projektu - E-Bezpečí*. Online. 2023. [cit. 2024-01-24]. Dostupné z: https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu.

4.2 Bílý kruh bezpečí

Počátky se datují již do roku 1991, kdy vzniklo „občanské sdružení Bílý kruh bezpečí“ z důvodu pomoci obětem trestných činů. V roce 1992 spolupracovali s Kanceláří prezidenta republiky v oblasti prevence kriminality a založili program „Žena a zločin“. Později se začali také zabývat tématem šikany na základních školách a postupně otevírali nové poradny v Olomouci, Brně, Ostravě či v Plzni. V roce 1996 se stali členem „The European Forum for Victim Services“. Začali spolupracovat s mnohými nadačními fondy a v jejich působnosti vznikly také dokumenty České televize o obětech kriminality. S nástupem internetu spustili v roce 2000 své první webové stránky. Od té doby se zapojili do nespočtu projektů, kampaní a otevírali stále více poraden. Začali se taky angažovat ve školení policistů v oblasti komunikace a kontaktu se zvlášť zranitelnými obětmi a pozůstalými. Další jejich významný milník nastal v roce 2015, kdy vznikla nonstop bezplatná linka pomoci obětem kriminality a domácího násilí s číslem 116 006.[32]

Bílý kruh bezpečí nabízí kompletní pomoc obětem trestných činů – od právních informací, psychologického a sociálního poradenství po praktické rady, tipy a informace. Toto sdružení však působí i na preventivní rovině, a to zejména aktivní účastí při tvorbě zákonů a legislativy prostřednictvím předkládání podnětů k zákonodárným iniciativám. Realizují přednášky, výcviky, semináře a konference v oblasti práva a sociálních otázek. Aktivně vytvářejí a realizují vlastní projekty a účastní se mezinárodních projektů ve spolupráci s nevládními organizacemi, státní správou a místní samosprávou v České republice. Spolupracují také na mezinárodní úrovni, a to zejména s Victim Support Europe.[33] Níže se lze podívat na slogan vydaný ke dvacátému výročí Bílého kruhu bezpečí.

[32] *Příběh BKB*. Online. 2021. [cit. 2024-01-24]. Dostupné z: https://www.bkb.cz/o-nas/timeline/.
[33] *Poslání a činnost.* Online. [cit. 2024-01-24]. Dostupné z: https://www.bkb.cz/o-nas/poslani-a-cinnost/.

Obrázek 4 - slogan ke dvacátému výročí Bílého kruhu bezpečí

4.3 Seznam se bezpečně

Internet přináší širokou škálu možností, ale bohužel nese i svá rizika. Je to bolestivě patrné v příběhu patnáctileté dívky, která v roce 2007 spáchala sebevraždu poté, co byly zveřejněny její intimní fotografie. S cílem předejít podobným tragédiím zahájila společnost Seznam.cz projekt „Seznam se bezpečně“, který se aktivně věnuje otázkám internetové bezpečnosti. Společnost nabízí mnoho materiálů a aktivit podporující prevenci a informovanost o nebezpečí na internetu. Jedná se například o filmy, které mají zvýšit povědomí o rozesílání intimních fotografií nebo filmy natočené podle pravdivé události, která se stala v Čechách, a to o zneužívání dětí skautskými vedoucími. Jejich pole působností je velmi různorodé a kreativní a zaměřené tak, aby upoutalo nejen dětskou pozornost. Příkladem je třeba pořádání divadelních představení ve spolupráci s pražským Studiem Ypsilon. Nabízejí také online podporu pro děti a dospělé a pro ty, kteří se chtějí vzdělávat doma, vydali knihu s názvem „Bezpečně na internetu“.[34]

[34] *Seznam se bezpečně - JSNS*. Online. [cit. 2024-01-24]. Dostupné z: https://www.jsns.cz/projekty/medialni-vzdelavani/bulletin-medialni-vzdelavani/predstavujeme/seznam-se-bezpecne.

4.4 Linka bezpečí

Linka bezpečí byla založena v roce 1994 jako druhá linka svého druhu v Evropě (první dětská linka byla ChildLine ve Velké Británii). V roce 2006 otevřeli chat Poradny, které pomáhaly dospívajícím řešit jejich problémy přes písemný kontakt. Jako první v ČR získali akreditaci pro výcvik krizové intervence. Ve spolupráci s CZ.NIC zastřešují evropský projekt „Safer internet“, který je zaměřen především na bezpečný pohyb a využívání sociálních sítí a internetu dospívajícími. Zabývají se také pasivní poradenskou formou, kterou realizují prostřednictvím podcastu „Na Tenké Lince“.

Linka bezpečí, z.s. má za cíl poskytovat kvalitní a snadno dostupnou pomoc dětem a studentům do 26 let na telefonním čísle 116 111, na e-mailu nebo chatu. Tato organizace se zaměřuje na poskytování krizové intervence, poradenství a prevence pro klienty po celé České republice. Současně se věnuje vzdělávání odborné veřejnosti, která pracuje s dětmi. Jejich závazkem je přispívat ke zlepšení celkové kvality života dětí. Jsou vzdělávací institucí, která realizuje několik akreditovaných výcviků a kurzů nejen pro osoby pracující s dětmi.[35]

Mezi jejich kurzy patří například souhrnný výcvik v telefonické krizové intervenci. Kurzy krizové intervence se zaměřují na techniky aktivního poslechu, empatii a vhodné komunikační strategie, jež jsou klíčové pro efektivní komunikaci s lidmi v krizových situacích. To pomáhá vytvářet důvěru a uklidňovat postižené osoby. Kurzy nabízejí vhodné postupy pro poskytování emocionální podpory a uklidňování lidí v krizi. To je zvláště důležité při řešení situací s emocionálním nebo psychologickým stresem, kde je klíčové být citlivý a empatický. Získání znalostí a dovedností v oblasti krizové intervence posiluje sebevědomí a profesionální jistotu. Účastníci jsou lépe vybaveni k řešení náročných situací a mohou se cítit pohodlněji při jejich řešení. Všechny tyto kurzy jsou akreditovány Ministerstvem práce a sociálních věcí, a stojí od dvou do dvaceti čtyř tisíc korun.[36]

[35] *Linka bezpečí | O nás*. Online. C1994-2024. [cit. 2024-01-24]. Dostupné z: https://www.linkabezpeci.cz/o-nas.
[36] *Linka bezpečí | Kurzy*. Online. C1994-2024. [cit. 2024-01-24]. Dostupné z: https://www.linkabezpeci.cz/o-nas.

Praktická část

5 Cíle výzkumného šetření

Cílem mého výzkumného šetření bylo vyhodnotit následující teze, které jsem navrhla v souvislosti s teoretickou částí mé bakalářské práce.

1. Analyzovat povědomí o rizicích na sociálních sítích;
2. Posoudit osobní zkušenosti respondentů;
3. Zhodnotit, zda si uživatelé na internetu dostatečně hlídají své soukromí;
4. Ověřit míru edukace;
5. Navrhnout doporučení o možných formách edukace s dostatečným hlídáním soukromí.

6 Výzkumné šetření

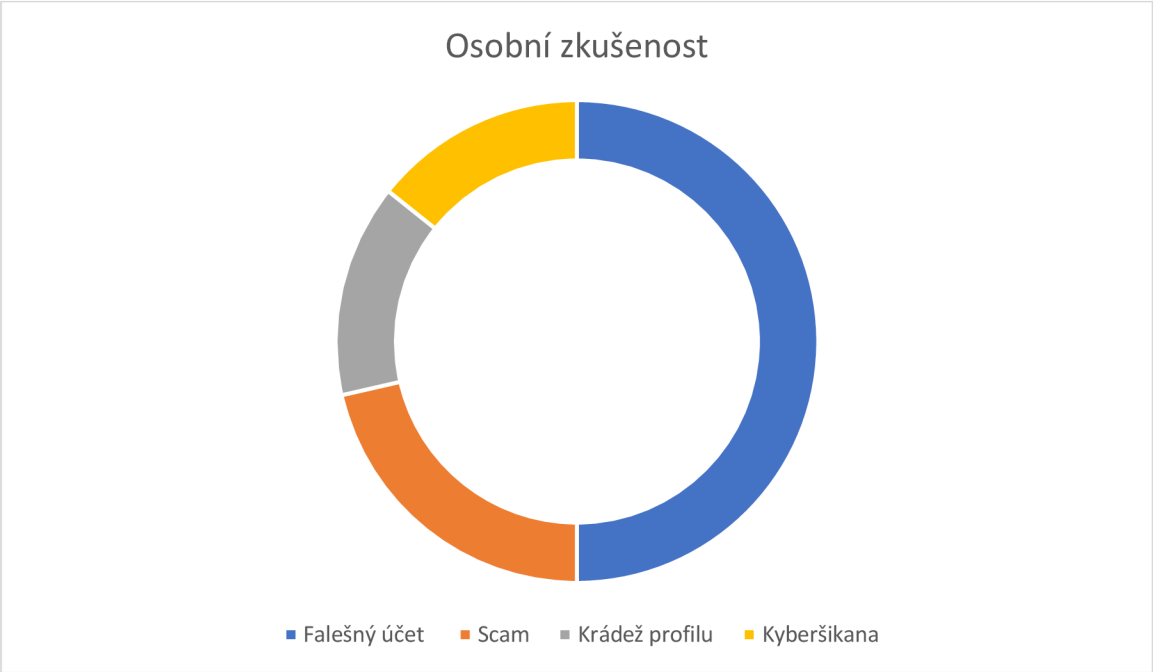
6.1 Obecné informace o používání sociálních sítí

Jako první bylo důležité vydefinovat základní informace o dotazovaných uživatelích v souvislosti s používáním sociálních sítí. Nikoho nejspíš nepřekvapí, že dnešní generace je každodenním uživatelem sociálních sítích. Tento fakt vyplynul hned na začátku rozhovorů. Všichni respondenti uvedli, že jsou uživateli na denní bázi a stráví na sociálních sítích i několik hodin denně, a to průměrně 3,6 hodiny.

Nejvíce preferovanou sociální sítí mezi účastníky provedeného průzkumu je jednoznačně Instagram, jehož popularita dosahuje až 100 % mezi respondenty. Na druhé příčce se umístil Facebook, avšak jeho využívání zaznamenalo pokles a v současnosti je využíván pouze 60 % dotázaných. Pokud bychom se podívali do minulosti, Facebook byl po dlouhou dobu neotřesitelným lídrem v oblasti sociálních médií. Nicméně s nástupem tzv. „generace Z“ dochází k postupnému úbytku zájmu o tuto platformu mezi staršími uživateli. I když 90 % respondentů uvedlo, že si na Facebooku založili svůj první profil, je zřejmé, že tato síť se stále více profiluje jako platforma pro starší generace, zatímco mladší generace preferuje jiné sociální sítě, jako je například Instagram. Tento trend může být způsoben řadou faktorů, včetně změny preferencí uživatelů, nových funkcí sociálních sítí a nárůstu obsahu cíleného na konkrétní skupiny.

6.2 Zkušenost

Četnost osobních zkušeností s různými formami zneužití nebo úniku dat a informací na sociálních sítích je značná. Naprosto všichni účastníci průzkumu potvrdili, že se v průběhu svého života setkali minimálně s jedním takovýmto incidentem, ať už na vlastní kůži či prostřednictvím svých známých. Nejčastějším způsobem zneužití osobních údajů je vytvoření falešného účtu, což se potvrdilo až u 70 % respondentů. Tento neoprávněný přístup k osobním informacím se obvykle soustředí na zneužití jména, příjmení a fotografie uživatele, čímž dochází k ohrožení jeho soukromí a bezpečnosti. Dalšími běžnými formami zneužití jsou například scam, krádež profilu a kyberšikana, s nimiž se setkalo 30 %, 20 % a 20 % zúčastněných respondentů. Tento druh zneužití osobních údajů může mít vážné důsledky, které zahrnují i finanční ztráty nebo emocionální újmu.



Obrázek 5 - nejpoužívanější hesla na sociálních sítích za období 2019 – 2021

Z mého průzkumu dále vyplývá, že u 40 % respondentů se setkalo se situací, kdy došlo k přímé krádeži nebo zneužití jejich osobních údajů. Tato zneužití se obvykle týkala krádeže identity přímo na sociálních sítích, což může mít vážné důsledky pro bezpečnost a soukromí dotyčné osoby. Dojde například k neoprávněnému použití osobních údajů, což může vést až k finančním podvodům, zneužití platebních údajů nebo jiným formám podvodu. V jednom případě jsme se setkali s kyberšikanou, což je forma agresivního chování a obtěžování na internetu. Tato situace může mít negativní dopad na psychické zdraví oběti, vyvolávající úzkost, stres a další emocionální obtíže. Je důležité, aby uživatelé sociálních sítí byli obezřetní a chránili své osobní údaje před neoprávněným použitím a zneužitím, aby se vyhnuli těmto rizikům.

6.3 Rizika

Rizik je na sociálních sítích spoustu, avšak i přesto se najdou jedinci, kteří si jich stále nejsou vědomi. Při ověřování povědomí respondentů o rizicích pouze jeden z účastníků odpověděl, že mu žádná rizika nehrozí. Ostatní si jsou rizik dostatečně vědomi a zazněly obavy například ze závislosti na sociálních sítích, sextingu, kyberšikany, fake účtů, zneužití dat, scamu nebo zneužívání fotografií.

Nejčastějším způsobem, s nímž se setkalo 70 % respondentů, bylo zneužívání osobních dat, informací a fotek prostřednictvím vytváření **fake účtů.** Tyto účty bývají často problematické a mají potenciál vytvářet negativní důsledky. Tento způsob útoku

se často využívá k záměrnému šíření dezinformací, šíření nenávisti nebo k napadání konkrétních jednotlivců nebo skupin. Fake účty mohou také sloužit k útokům na soukromí uživatelů a k šíření škodlivých obsahů. Je důležité být obezřetný při identifikaci a vyhýbat se interakcím s podezřelými nebo neznámými účty, aby se minimalizovalo riziko manipulace, zneužití nebo poškození reputace.

Scam neboli podvod je způsob, jakým se jednotlivci nebo organizace pokoušejí získat neoprávněný přístup k osobním údajům, finančním prostředkům nebo jiným cenným informacím od svých obětí. Tento způsob podvádění se často vyskytuje online prostřednictvím e-mailů, telefonních hovorů, textových zpráv nebo sociálních médií a setkalo se s ním 30 % respondentů. Scam může nabízet falešné investiční příležitosti, falešné loterie, falešné zprávy o výhře, žádosti o osobní údaje pod záminkou ověření identity nebo falešné prodeje zboží nebo služeb. Cílem je často přesvědčit oběť, aby poskytla citlivé informace nebo provedla platbu, která by mohla být zneužita. Je důležité být obezřetný a nepodléhat podezřelým nabídkám a raději tyto situace nahlásit správným orgánům či subjektům.

Krádež profilu na sociálních sítích je způsob, jakým se útočníci neoprávněně zmocní přístupu k účtu někoho jiného. Toto riziko ve své výpovědi uvedli dva respondenti a jeden z nich se zmínil o tom, že ukradený účet byl přímo jeho. Uvedl, že účet mu byl ukraden pomocí škodlivého softwaru a že snahy o jeho navrácení byly marné. Krádež účtu může být realizována různými způsoby, včetně phishingu, kdy útočníci vytvoří falešnou webovou stránku nebo odesílají falešné e-maily, které žádají uživatele o zadání svého uživatelského jména a hesla. Další metodou může být použití škodlivého softwaru, který získá přístupové údaje k účtu, nebo je útočníci mohou získat pomocí manipulace s uživatelem tak, aby jim poskytl své přihlašovací údaje. Po získání přístupu mohou útočníci ukrást citlivá data, zveřejňovat nevhodný obsah nebo se vydávat za osobu, jejíž účet byl odcizen.

Dále bych se chtěla věnovat riziku, které je podle mě jedno z nejhorších, jelikož jeho následky mohou mít velmi škodlivý dopad na psychické zdraví jedince. Polovina respondentů uvedla, že se za svůj život alespoň jednou setkala se **sextingem**, což znamená, že každý druhý byl svědkem zneužití intimních fotografií jiných osob, nebo byl dokonce tím, kdo tyto explicitní fotografie posílal. Tento trend se stává stále běžnějším, zejména mezi mladými lidmi. Sextingové zprávy mohou být nechtěně či

chtěně sdíleny s neautorizovanými osobami nebo se můžou stát předmětem šikany nebo vydírání. Z důvodu možných negativních důsledků je důležité, aby uživatelé byli obezřetní při sdílení intimních materiálů a měli na paměti, že v online prostředí není soukromí vždy zaručeno. Mladí lidé by měli být edukováni o rizicích sextingu a také způsobech, jak chránit své soukromí a integritu online.

Závažným problémem v online prostředí je **kyberšikana**, která může zahrnovat různé formy šikany, vydírání nebo hanobení prostřednictvím internetu nebo mobilních zařízení. Je spojena s emocionálním stresem, úzkostí a může mít negativní dopady na psychické zdraví jednotlivců. Z mého průzkumů vyplývá, že se alespoň jednou s kyberšikanou setkali dva z deseti respondentů, což naznačuje rozšířenost tohoto problému v online komunitách. Ti, kteří se s kyberšikanou setkali, uváděli pocit bezmoci a neschopnosti účinně se bránit proti šikaně. Zážitek kyberšikany u obou respondentů vyvolal silné emoční reakce, jako je strach, úzkost, vztek nebo smutek. Jeden dotazovaný dokonce trpěl narušením spánku, sníženým sebevědomím a sebedůvěrou a začal pochybovat o sobě a své hodnotě. Kyberšikana u něj způsobila i fyzické příznaky, jako bolesti hlavy, zažívací potíže a svalové napětí. Důsledky kyberšikany mohou být dlouhodobé a ovlivnit celkovou kvalitu života oběti. Je důležité, aby oběti kyberšikany měly přístup k podpoře a profesionální pomoci, která jim pomůže zvládnout trauma a navrátit se k pocitu bezpečí a pohody.

Dva respondenti jako další možné riziko uvedli **závislost** na sociálních sítích, jež se projevuje nadměrným používáním těchto platforem. Lidé často tráví na sociálních sítích příliš mnoho času, což může vést k omezení jejich produktivity v jiných činnostech. Samotná závislost je hodně ošemetné téma, jelikož se nejspíš týká většiny z nás. Dnešní mladá generace prakticky odkojená na telefonech neudělá bez svého smartphonu většinou ani krok. Berou si ho do obchodu, do školy, na toaletu a většina jej má u sebe celou noc. Celkově může závislost na sociálních sítích negativně ovlivnit fyzické a duševní zdraví jedince. Je důležité si být vědomý rizik spojených s nadměrným používáním těchto platforem a aktivně pracovat na udržení vyváženého vztahu s online světem.

Další riziko, na kterém se shodla téměř polovina účastníků, je **srovnávání se s nerealistickými ideály**. Tento „trend“ postihuje hlavně mladší uživatele, jelikož nemají ještě zcela utvořenou představu o tom, co je přirozené a co už je daleko za

hranicí reálného. Fenomén nerealistické krásy stojí za úspěchy mnoha influencerek a influencerů. Uživatelé často vidí pouze vybrané a upravené momenty života ostatních, což může vést k iluzi dokonalosti a nedostatku vlastních úspěchů. Tento jev může vyvolat pocit nedostatečnosti a nespokojenosti s vlastním životem. Lidé se často porovnávají se zprostředkovanými ideály krásy, úspěchu a štěstí, což může vést k nízkému sebehodnocení a narušenému sebevědomí. Srovnávání se s nerealistickými ideály na sociálních sítích může také přispět k emocionálnímu stresu a úzkosti. Neustálé vidění zdánlivě dokonalých životů ostatních může vyvolat pocity izolace a osamělosti u jednotlivců, kteří se necítí, že dosahují stejné úrovně štěstí a úspěchu. Je důležité si být vědomý toho, že prezentované životy na sociálních sítích nejsou vždy reprezentativním obrazem skutečnosti. Udržování zdravé perspektivy a uvědomění si této skutečnosti může pomoci minimalizovat negativní dopady srovnávání se s nerealistickými ideály online.

Přístup mládeže k nevhodnému obsahu je jeden z největších problému nezletilých uživatelů sociálních sítí. Tento fakt si uvědomují také sami respondenti, jelikož 70 % dotazovaných toto riziko při strukturovaném rozhovoru zmínilo. I přes to, že je například Facebook nebo TikTok až od 13 let, bychom na těchto platformách našli spoustu jedinců, kteří této věkové hranice ještě nedosáhli. Toto však není žádná novinka, při řízném rozhovoru sedm z deseti lidí odpovědělo, že si první účet založili dříve než ve 13 letech. V dnešní době ale štafetu přebírá TikTok. Platforma určená převážně k nahrávání krátkých videí v posledních letech raketově vystřelila a s ní i počet videí nevhodných pro nezletilé. Uveďme si jako příklad Adélu Pulcovou, také známou jako Shopaholic Adél. Tato influencerka je ukázkových příkladem sdílení vulgárního obsahu a naprosté finanční negramotnosti. Dostat se na její účty na sociálních sítích lze bez sebemenšího problému a kvanta často bezpředmětného obsahu máte na dosah ruky. Nevhodný vliv Shopaholic Adel může být značný. Když uživatelé pravidelně vidí, jak Adel utrácí velké množství peněz za nepotřebné věci, mohou si toto chování osvojit jako normální. To může vést k tomu, že budou mít zkreslené vnímání hodnoty peněz a materiálních statků. Adel může také představovat nevhodné vzory pro děti v oblasti financí a zodpovědného nakupování a v budoucnu to může vést k problémům s řízením financí.

I přes všechna známá rizika má každý z respondentů veřejně dostupnou fotografii jich samotných, která může být zneužita například jako podklad pro založení

fake účtu. Své pravé jméno a příjmení nemají veřejné dva z oslovených. Pět z deseti lidí se vyjádřilo tak, že mají veřejný svůj e-mail. Jeden člověk také telefonní číslo. Dokonce se našli i tací, kteří mají zveřejněnou svou reálnou polohu v reálném čase. A pouze šest lidí si myslí, že jejich veřejně dostupné informace mohou být zneužity.

6.4 Opatření

Správné nastavení účtu na sociálních sítích je klíčové pro ochranu osobních údajů před zneužitím, avšak přesto pouze 40 % respondentů zabezpečuje své účty tímto způsobem. Každá sociální síť má různé možnosti nastavení soukromí, které vám umožňují kontrolovat, kdo může vidět vaše příspěvky, fotografie a informace o profilu. Je důležité pravidelně kontrolovat a upravovat tato nastavení podle vašich preferencí a potřeb a nesdílet na sociální sítě informace, jež by mohly být zneužity někým jiným.

Velmi důležitým faktorem jsou také **zařízení, přes která se přihlašujeme**. V dnešní době se téměř každý připojuje k sociálním sítím přes svůj chytrý telefon. Sedm respondentů uvedlo, že mimo svůj telefon používají také stolní počítač či notebook. Dva používají tablet a jeden PlayStation. Proto je důležité dbát na zabezpečení našich zařízení a vždy se zamyslet, pokud se budeme chtít přihlásit z jiného zařízení než z toho svého.

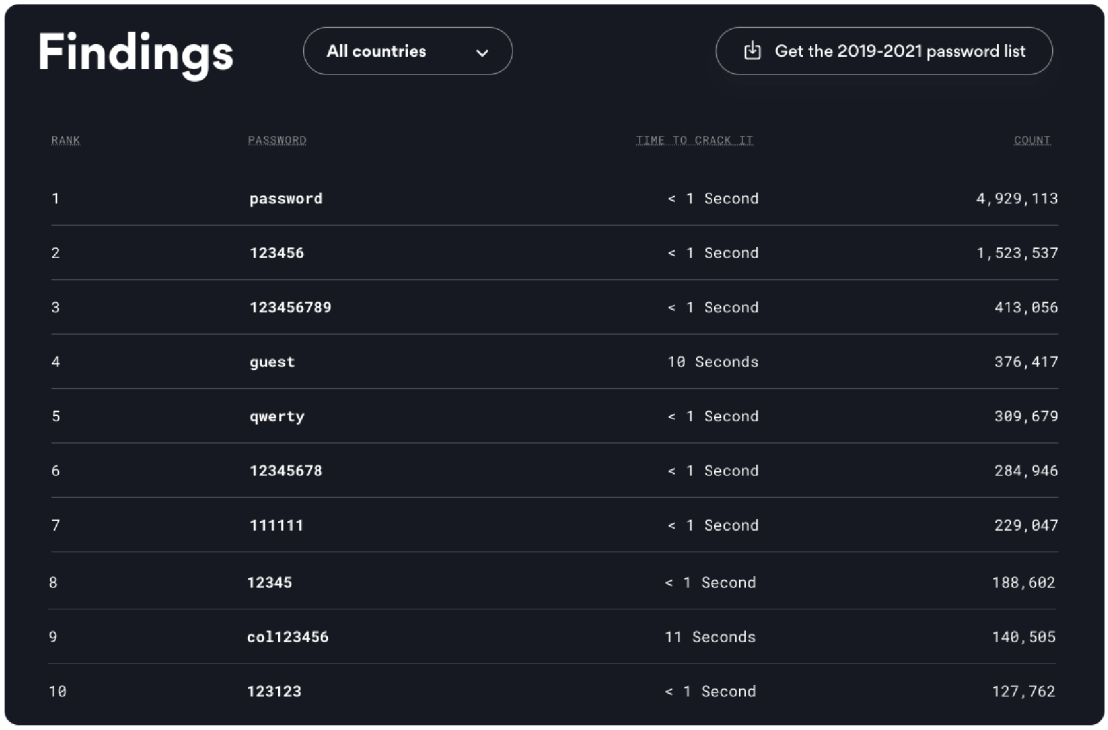
Dvoufázové ověření je bezpečnostní postup, který vyžaduje, aby uživatel při přihlašování nebo provádění citlivých operací prokázal svou identitu pomocí dvou různých faktorů. Tyto faktory mohou zahrnovat něco, co uživatel ví (například heslo), či něco, co uživatel vlastní (například mobilní telefon). Princip dvoufázového ověření spočívá v tom, že kromě klasického přihlašovacího údaje (jako je heslo) uživatel musí poskytnout ještě druhý, nezávislý faktor ověření, aby se mu umožnil přístup do systému nebo k provedení citlivých akcí. Tím se zvyšuje bezpečnost, protože útočník by musel získat oba faktory, což je mnohem obtížnější než získání pouze hesla. Tento bezpečnostní prvek využívá polovina respondentů.

Přestože **antivir** používá jen 30 % respondentů, je jeho užití klíčové pro ochranu osobních údajů před zneužitím. Antivirové programy mohou identifikovat a odstranit škodlivý software, který může být nainstalován na počítači nebo mobilním zařízení a který by mohl získávat nebo poškozovat osobní údaje. Antivirový software může chránit osobní údaje před různými hrozbami, včetně virů, spywaru, ransomwaru a dalších typů malwaru. Mnoho antivirových programů také nabízí funkce pro ochranu

před phishingovými útoky, které mohou mít za cíl získat citlivé informace, jako jsou hesla nebo bankovní údaje. Uživatelé by měli také být opatrní při stahování a instalaci aplikací a souborů z internetu a měli by se vyhýbat klikání na podezřelé odkazy nebo otevírání příloh v e-mailových zprávách od neznámých odesílatelů.

6.4.1 Hesla

Jedním ze základních stavebních kamenů zabezpečení účtu jsou **silná hesla**. Hesla by se měla skládat z velkých a malých písmen, čísel a znaků. Devět z deseti lidí sdělilo, že takto silná hesla používají na všech svých sociálních sítích. Nikdy by se jako hesla neměla používat vaše jména, či jména domácích mazlíčků. Lidé často používají předvídatelná hesla. Podle průzkumu NordPass bylo mezi lety 2019 až 2021 nejpoužívanějším heslem slovo „password“, které v překladu z anglického jazyka znamená „heslo“. Toto heslo používalo bezmála skoro pět milionů účtů. Zkušenému hackerovi by přitom netrvalo ani sekundu, než by toto heslo prolomil. Níže se lze podívat na celou statistiku nejpoužívanějších hesel. Velmi oblíbená jsou také po sobě jdoucí čísla.[37]



Obrázek 6 – Nejpoužívanější hesla za rok 2019 - 2021

[37] SVATENKO, Inna. *Jak vymyslet silné heslo: užitečné návyky pro bezpečnost na Internetu* | Laba Czech 🐰. Online. Roč. 2023. [cit. 2024-02-12]. Dostupné z: https://l-a-b-a.cz/blog/735-nejoblibenejsim-heslem-roku-2022-bylo-heslo-ktere-lze-prolomit-behem-vteriny.

Pravidelná změna hesel je další z preventivních kroků a opatření, které však dělá pouze jedna pětina oslovených. Pravidelně měnit hesla na sociálních sítích je důležité z důvodu zvýšení bezpečnosti účtu a ochrany osobních údajů. Častá změna hesla může snížit riziko prolomení účtu a neoprávněného přístupu k osobním informacím. S rychlým rozvojem technologií a metod kybernetických útoků je důležité udržovat krok a přizpůsobovat své zabezpečení. Pravidelná změna hesla také může chránit před případnými útoky zneužití starých hesel, která mohla být ukradena v minulosti. Změna hesla může také pomoci minimalizovat škody v případě, že dojde k úniku hesla z účtu. Díky pravidelnému měnění hesla můžete lépe chránit své soukromí a osobní údaje a udržet svůj účet na sociálních sítích v bezpečí.

Na každém účtu by měla být **separátní hesla**, jelikož to snižuje riziko, že útočník získá přístup k dalším účtům téže osoby. Pouze tři účastníci uvedli, že mají na každé sociální síti jiná hesla. Rozdílné přihlašovací údajena různých účtech ztěžují útočníkům možnost proniknutí do dalších účtů, pokud by jeden z nich byl napaden. Každý účet by měl mít unikátní heslo, aby byla zajištěna co nejvyšší úroveň bezpečnosti. Všichni uživatelé by měli mít na sociálních sítích rozdílná hesla z důvodu zvýšení bezpečnosti svých účtů. Použití stejného hesla na různých platformách zvyšuje riziko útoku, protože pokud je heslo ukradeno na jedné sociální síti, může být použito k neoprávněnému přístupu k dalším účtům.

6.5 Edukace

Vzdělávání o bezpečnosti na sociálních sítích je klíčové pro prevenci rizik spojených s online prostředím. Tato edukace zahrnuje informování uživatelů o nebezpečích, která mohou na sociálních sítích číhat, a poskytování nástrojů a znalostí, jak se chránit. To může zahrnovat výuku o důležitosti silných hesel, ochraně osobních údajů, rozpoznání kyberšikany a podvodu a zodpovědném sdílení obsahu. Edukace by měla být dostupná pro všechny věkové skupiny, od dětí po dospělé, a měla by být průběžná, jelikož hrozeb stále přibývá. Nejčastější formou edukace pro osoby do dvaceti šesti let jsou semináře a přednášky v rámci školy, kterých se zúčastnila polovina dotazovaných. Čtyři z nich k tomu pravidelně čtou také články na internetu a jeden respondent odpověděl, že své vzdělání získává z odborných knížek a literatury.

Dle mého názoru je edukace u většiny respondentů nedostatečná. Edukace o bezpečnosti informací na sociálních sítích může představovat závažné riziko pro

uživatele. Čtyři z deseti účastníků rozhovoru nemají dostatečné povědomí o tom, jak chránit své osobní údaje nebo jak rozpoznat potenciální nebezpečné situace online. To vede k tomu, že se stanou snadnou kořistí pro kybernetické útočníky, kteří mohou zneužít jejich údaje nebo je vystavit různým online hrozbám. Nedostatek vhodné edukace také způsobuje, že uživatelé nejsou schopni rozpoznat phishingové útoky, šíření dezinformací nebo kyberšikanu. Neznalost rizik spojených se sociálními sítěmi může vést k tomu, že lidé sdílejí příliš mnoho osobních informací, což může mít negativní dopady na jejich soukromí a bezpečnost. Je důležité, aby uživatelé byli dostatečně informováni o bezpečnostních opatřeních, která mohou přijmout, aby chránili své účty a osobní údaje. Tato edukace by měla zahrnovat různé tipy a triky pro bezpečné chování online, informace o možných hrozbách a nácvik identifikace podezřelých aktivit či zpráv na sociálních sítích.

7 Vyhodnocení

Na základě získaných dat z vedených strukturovaných rozhovorů mohu vyhodnotit, že všichni dotazovaní tráví na svých sociálních sítích několik hodin denně bez ohledu na pohlaví a bez svých chytrých telefonů neudělají ani krok. V dnešní době, kdy je všechno více a více digitalizované, se není čemu divit, jelikož lidé ve svých telefonech mají doklady nebo bankovní karty. Příkladem digitalizace může být například nová aplikace eDoklady, kterými se od 20. ledna můžete prokazovat u Ústředních správních úřadů. Digitalizace dokladů je krok kupředu, ale opět nutí lidi, aby měli svůj telefon vždy po ruce. Výsledky zkoumání naznačují významnou dominanci Instagramu jakožto nejpoužívanější sociální sítě mezi respondenty. Sto procent respondentů uvedlo, že používá Instagram, což ukazuje na jeho vysokou popularitu a rozšíření mezi uživateli. Na druhém místě se umístil Facebook, který používá 6 z 10 respondentů, což naznačuje mírný pokles popularity oproti Instagramu. Mezi další často používané sociální sítě patří Snapchat, TikTok a WhatsApp, avšak výzkum neposkytuje podrobnější informace o jejich použití. Tato data ukazují na různorodost sociálních sítí, které jsou mezi respondenty oblíbené, a zdůrazňují důležitost Instagramu jako hlavní platformy pro sociální interakce mezi generací Z.

Výsledky naznačují, že respondenti jsou si vědomi rizik spojených s informacemi na sociálních sítích. Tato zjištění svědčí o zvýšené obezřetnosti a uvědomělosti respondentů ohledně možných hrozeb a nebezpečí spojených s uveřejňováním osobních informací na online platformách. Tento poznatek může naznačovat vzrůstající důraz na ochranu osobních údajů a snahu minimalizovat rizika vystavení se kybernetickým hrozbám. Vedle toho je důležité podporovat další vzdělávání a osvětu v oblasti kybernetické bezpečnosti, aby uživatelé mohli lépe porozumět rizikům a naučit se, jak se chránit před potenciálními nebezpečími na sociálních sítích.

Dále je zřejmé, že respondenti si nedostatečně hlídají obsah, jenž sdílejí na sociálních sítích. Tato zjištění poukazují na nedostatečnou uvědomělost či nedbalost ohledně ochrany osobních údajů a soukromí online. Nedostatek pozornosti k obsahu, který je sdílen na sociálních sítích, může zvyšovat riziko vystavení se kybernetickým hrozbám, jako je například krádež identity, kyberšikana nebo neoprávněný sběr osobních údajů. Tato situace zdůrazňuje potřebu zvýšené osvěty a edukace ohledně bezpečného chování na sociálních sítích a důležitosti ochrany osobních údajů online.

Výsledky dále naznačují, že 100 % respondentů se alespoň jednou setkalo se zneužitím osobních údajů na sociálních sítích. Tato skutečnost poukazuje na rozšířenost problému ochrany osobních údajů a bezpečnosti online prostředí. Zneužití osobních údajů může mít různé formy, včetně vytvoření fake účtu, scamu, kyberšikany nebo krádeže profilu. Tato zjištění zdůrazňují potřebu posílení opatření pro ochranu osobních údajů a zvýšení povědomí o bezpečném chování na sociálních sítích. Je nezbytné poskytnout uživatelům nástroje a znalosti, které jim umožní chránit své osobní údaje a minimalizovat riziko jejich zneužití online.

Na základě získaných dat jsem vyhodnotila, že většina respondentů má nedostačující edukaci v oblasti bezpečnosti na internetu. Tento fakt poukazuje na potřebu posílení osvěty a vzdělávání v této oblasti, aby uživatelé byli lépe vybaveni k rozpoznání a minimalizaci rizik spojených s online aktivitami. Nedostatečná edukace může vést k neuváženému sdílení osobních údajů, klikání na podezřelé odkazy nebo spoléhání se na nezabezpečené hesla. Je třeba investovat do programů a kampaní zaměřených na zvyšování povědomí o bezpečnosti na internetu, aby uživatelé měli dostatečné znalosti k ochraně svého soukromí a ohledně bezpečnosti online.

7.1 Doporučení

Ze získaných výsledků je jasné, že je nezbytné zaměřit se na poskytování lepší edukace o bezpečnosti na internetu pro veřejnost, zejména pro mladé lidi, kteří jsou často zranitelní vůči kybernetickým hrozbám. To může zahrnovat vytvoření komplexních edukačních programů, které budou zahrnovat informace o bezpečnosti online, kybernetických rizicích a ochraně soukromí. Tyto programy by měly být přístupné v různých formátech a vhodné pro různé věkové skupiny. Školy a vzdělávací instituce by měly hrát klíčovou roli v poskytování této edukace. Měly by začlenit osnovy týkající se bezpečnosti online a ochrany soukromí do svého vzdělávacího systému na všech úrovních vzdělávání. To by mohlo zahrnovat výuku o tom, jak správně používat sociální sítě, jak rozpoznat rizikové situace online a jak chránit své osobní údaje. Veřejnost by měla být informována o důsledcích neopatrného chování online a o tom, jaká rizika mohou vzniknout v důsledku nedostatečné ochrany osobních údajů. To může zahrnovat informační kampaně, bezplatné workshopy a školení, které budou zdůrazňovat důležitost bezpečnosti na internetu a zároveň poskytovat praktické tipy a návody pro bezpečné chování online.

Lidé by měli být opatrní při sdílení osobních údajů na sociálních sítích, aby chránili svou soukromí a bezpečnost online. Mezi informace, které by neměli sdílet, patří jejich domovská adresa, číslo sociálního pojištění, bankovní údaje nebo jakékoli další citlivé finanční informace. Dalšími informacemi, které by měli lidé zvažovat, zda je sdílet, jsou detaily o svých cestách, plány na dovolenou nebo příspěvky, které by mohly odhalit jejich polohu v reálném čase. To může zvyšovat riziko domácích krádeží nebo útoků na jejich osobní bezpečnost. Kromě toho by měli lidé být opatrní při sdílení osobních fotografií a videí, zejména těch, které obsahují děti nebo další citlivé informace. Také by měli zvážit, zda chtějí sdílet informace o svém osobním životě, vztazích nebo pracovních záležitostech, jež by mohly být zneužity nebo interpretovány negativně. Vědomé rozhodování o tom, které informace jsou vhodné ke sdílení a které ne, může pomoci chránit jednotlivce před kybernetickými hrozbami a nechtěnými důsledky sdílení osobních údajů online.

Závěr

Závěr této bakalářské práce představuje komplexní zhodnocení výzkumných zjištění a následných doporučení, která vyplynula z analýzy prováděného průzkumu. V rámci tohoto průzkumu byla identifikována řada klíčových aspektů týkajících se bezpečnosti informací na sociálních sítích a povědomí uživatelů o rizicích, která s sebou jejich používání nese.

Jedním z hlavních zjištění je, že uživatelé sociálních sítí mají různorodé zkušenosti s riziky spojenými s jejich používáním. Respondenti vykazují určitou úroveň povědomí o možných nebezpečích, jako jsou například zneužití osobních údajů, kyberšikana či krádeže identity. Nicméně, přestože je povědomí o těchto rizicích relativně vysoké, je zde stále prostor pro zlepšení v oblasti ochrany soukromí a osobních informací.

Jedním z klíčových aspektů, na který by měla být kladená pozornost, je nedostatečná ochrana osobních údajů a soukromí uživatelů. Respondenti často sdílejí citlivé informace a obrázky bez dostatečného uvědomění si rizik spojených s jejich zveřejněním. Tento trend je závažným indikátorem potřeby zlepšení povědomí a vzdělávání v oblasti ochrany soukromí na sociálních sítích.

Dalším důležitým zjištěním je nedostatečná úroveň edukace uživatelů v oblasti bezpečnosti na internetu. Respondenti vykazují omezené povědomí o nejnovějších bezpečnostních hrozbách a nejlepších postupech pro ochranu svých účtů a dat. Z tohoto důvodu je nezbytné zlepšit edukační programy a informační kampaně, které budou cílit na zvýšení povědomí a znalostí v této oblasti. Na základě získaných výsledků je tedy nutné se zaměřit na posílení edukačních iniciativ a prevence rizik spojených s používáním sociálních sítí. To zahrnuje jak individuální opatření, jako je zlepšení povědomí a edukace uživatelů, tak i kolektivní snahy, jako je posílení bezpečnostních opatření na straně poskytovatelů sociálních sítí.

Pro ověření a podporu těchto zjištění by mohlo být vhodné provést další výzkum, který by zahrnoval rozsáhlejší kvantitativní analýzu a širší vzorek respondentů. Kombinace různých metod výzkumu by poskytla komplexní a vyváženější pohled na problematiku bezpečnosti na sociálních sítích a umožnila by efektivnější navrhování opatření pro ochranu uživatelů.

Seznam použité literatury

Monografie

1. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-34-8.
2. KOŽÍŠEK, Martin a PÍSECKÝ, Václav. *Bezpečně n@ internetu: průvodce chováním ve světě online.* Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

Zákonná úprava a interní akty řízení

1. *Národní strategie kybernetické bezpečnosti České republiky na období let 2021 až 2025*. [online]. [cit. 30. 11. 2023]. Dostupné z: http://narodni_strategie_kb_2020-2025_ cr (1).pdf
2. *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).* In: 2016.

Webové stránky a elektronické zdroje

1. ZEMAN, Petr. *Česká bezpečnostní terminologie: Výklad základních pojmů*. Online. [cit. 2023-12-05]. Dostupné z: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048. Str. 13
2. *Sociální sítě - INTERNETEM BEZPEČNĚ*. Online. [cit. 2023-12-05]. Dostupné z: view-source: https://www.internetembezpecne.cz/internetem-bezpecne/socialni-media/socialni-site/.
3. *Co je to kyberprostor? - Správa.sítě.eu*. Online. 2022. [cit. 2023-12-05]. Dostupné z: view-source: https://www.sprava-site.eu/kyberprostor/.
4. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Riziko - Ministerstvo vnitra České republiky.* Online. 2023, 2023. [cit. 2023-11-29]. Dostupné z: https://www.mvcr.cz/clanek/riziko.aspx
5. *Kyberšikana - INTERNETEM BEZPEČNĚ*. Online. C2018. [cit. 2024-01-19]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/.

6. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Hrozba*. [online]. [cit. 28. 11. 2023]. Dostupné z: http://www.mvcr.cz/clanek/hrozba.aspx
7. Co jsou to kybernetické hrozby. *Kybernetická bezpečnost | Aptien*. Online. 2023. [cit. 2023-12-05]. Dostupné z: view-source: https://aptien.com/cs/kb/articles/what-are-cybersecurity-threats.
8. *Sociální sítě: Přehled, seznam a žebříček největších a nejoblíbenějších*. Online. [cit. 2024-01-15]. Dostupné z: https://sitevhrsti.cz/socialni-site/.
9. *23 Top Social Media Sites for Your Brand in 2024, Ranked*. Online. 2023. [cit. 2024-01-15]. Dostupné z: view-source: https://buffer.com/library/social-media-sites/.
10. *Facebook: Getting Started with Facebook*. Online. [cit. 2024-01-16]. Dostupné z: view-source: https://edu.gcfglobal.org/en/facebook101/getting-started-with-facebook/1/.
11. *Facebook | History, Features, Description, & Facts | Britannica*. Online. 2023. [cit. 2024-01-16]. Dostupné z: https://www.britannica.com/topic/Facebook.
12. LEPEŠKOVÁ, Bc. Lenka. *Facebook jako bezpečnostní hrozba*. Diplomová práce. Brno: Masarykova univerzita, 2011. [cit. 2024-02-12].
13. *YouTube | Britannica*. Online. 2023. [cit. 2024-01-17]. Dostupné z: https://www.britannica.com/topic/YouTube.
14. *What is WhatsApp?* Social Media Marketing Definitions - SocialBee. Online. C2023. [cit. 2024-01-17]. Dostupné z: https://socialbee.com/glossary/whatsapp/.
15. *Jaké informace WhatsApp se společnostmi Meta sdílí?* | Centrum nápovědy pro WhatsApp. Online. C2024. [cit. 2024-01-17]. Dostupné z: https://faq.whatsapp.com/1303762270462331/?locale=cs_CZ.
16. I*nstagram | History, Features, Description, & Facts | Britannica*. Online. 2023. [cit. 2024-01-16]. Dostupné z: https://www.britannica.com/topic/Instagram.
17. *TikTok: What It Is, How It Works, and Why It's Popular*. Online. 2023. [cit. 2024-01-16]. Dostupné z: https://www.investopedia.com/what-is-tiktok-4588933.
18. Národní úřad pro kybernetickou a informační bezpečnost. *Aplikace TikTok představuje bezpečnostní hrozbu*. Online. 2023. [cit. 2024-01-16]. Dostupné z: https://nukib.gov.cz/cs/infoservis/hrozby/1941-aplikace-tiktok-predstavuje-bezpecnostni-

hrozbu/?fbclid=IwAR22tQZQXC6EyXEuPCIAQPzZRgm7en7LaHQNhpdtDNmN3nHfdTK1_TaHRQ8.

19. *X | Company, History, Twitter, Elon Musk, & Uses | Britannica*. Online. 2024. [cit. 2024-01-24]. Dostupné z: https://www.britannica.com/topic/Twitter.
20. *Pravidla pro bezpečné surfování na sociálních sítích – KYBEZ*. Online. 2020. [cit. 2024-01-17]. Dostupné z: https://kybez.cz/10-pravidel-pro-bezpecne-surfovani-na-socialnich-sitich/.
21. *Co jsou to osobní údaje? - Evropská komise*. Online. [cit. 2024-01-17]. Dostupné z: https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_cs.
22. CONFESSORE, Nicholas. *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far - The New York Times.* Online. The New York Times. 2018, roč. 2018. [cit. 2024-02-12]. Dostupné z: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.
23. *What Is Data Theft? Definition, Examples & More | Proofpoint US*. Online. [cit. 2024-01-19]. Dostupné z: https://www.proofpoint.com/us/threat-reference/data-theft.
24. *The 10 Types of Cyberbullying - Blog*. Online. 2023. [cit. 2024-01-23]. Dostupné z: https://blog.securly.com/10/04/2023/the-10-types-of-cyberbullying/.
25. *How to Prevent Cyberbullying*. Online. 2022. [cit. 2024-01-24]. Dostupné z: https://www.verywellfamily.com/how-to-prevent-cyberbullying-5113808.
26. *Informace o projektu - E-Bezpečí*. Online. 2023. [cit. 2024-01-24]. Dostupné z: https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu.
27. *Příběh BKB.* Online. 2021. [cit. 2024-01-24]. Dostupné z: https://www.bkb.cz/o-nas/timeline/.
28. *Poslání a činnost*. Online. [cit. 2024-01-24]. Dostupné z: https://www.bkb.cz/o-nas/poslani-a-cinnost/.
29. *Seznam se bezpečně* - JSNS. Online. [cit. 2024-01-24]. Dostupné z: https://www.jsns.cz/projekty/medialni-vzdelavani/bulletin-medialni-vzdelavani/predstavujeme/seznam-se-bezpecne.
30. *Linka bezpečí | O nás*. Online. C1994-2024. [cit. 2024-01-24]. Dostupné z: https://www.linkabezpeci.cz/o-nas.

31. *Linka bezpečí | Kurzy*. Online. C1994-2024. [cit. 2024-01-24]. Dostupné z: https://www.linkabezpeci.cz/o-nas.
32. SVATENKO, Inna. *Jak vymyslet silné heslo: užitečné návyky pro bezpečnost na Internetu | Laba Czech*. Online. Roč. 2023. [cit. 2024-02-12]. Dostupné z: https://l-a-b-a.cz/blog/735-nejoblibenejsim-heslem-roku-2022-bylo-heslo-ktere-lze-prolomit-behem-vteriny.

Seznam obrázků a tabulek