ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

MASARYKŮV ÚSTAV VYŠŠÍCH STUDIÍ

BAKALÁŘSKÁ PRÁCE

Kyberbezpečnost – rizika komunikace na síti

Cybersecurity – risks of network communication

2024

Kristýna Kolaříková

Studijní program: Učitelství odborného výcviku a praktického vyučování

Vedoucí práce: Ing. Petr Svoboda Ph.D., ING.PAEG.IGIP

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Kolaříková** Jméno: **Kristýna** Osobní číslo: **511342**

Fakulta/ústav: **Masarykův ústav vyšších studií**

Zadávající katedra/ústav: **Institut pedagogických a psychologických studií**

Studijní program: **Učitelství praktického vyučování a odborného výcviku**

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Kyberbezpečnost – rizika komunikace na síti

Název bakalářské práce anglicky:

Cybersecurity – risks of network communication

Pokyny pro vypracování:

Tématem bakalářské práce je kybernetická bezpečnost a rizika komunikace na síti. V teoretické části popisuji hlavní zásady zajištění ochrany informací a pravidla pro bezpečné používání prostředků výpočetní informační techniky. Rozeberu v teoretické části i jednotlivé rizika na síti. V empirické části bude obsahovat výsledky z dotazníkového šetření jehož cílem je zjistit, s jakými bezpečnostními riziky se uživatelé setkali a zda mají negativní zkušenost.

Seznam doporučené literatury:

Kybernetická (ne)bezpečnost. Problematika bezpečnosti v kyberprostoru, Sedlák P., Konečný M. a kol., 2021, ISBN 978-80-7623-068-2. SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8. ČERNÁ, Alena. Kyberšikana: průvodce novým fenoménem. Praha: Grada Publishing, a.s., 2013. ISBN 978-80-210-6374-7.

Jméno a pracoviště vedoucí(ho) bakalářské práce:

Ing. Petr Svoboda, Ph.D., ING.PAED.IGIP Masarykův ústav vyšších studií ČVUT v Praze

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) bakalářské práce:

Datum zadání bakalářské práce: **08.12.2023** Termín odevzdání bakalářské práce: **24.06.2024**

Platnost zadání bakalářské práce: _____

Ing. Petr Svoboda, Ph.D., ING.PAED.IGIP	doc. Ing. David Vaněček, Ph.D.	prof. PhDr. Vladimíra Dvořáková, CSc.
podpis vedoucí(ho) práce	podpis vedoucí(ho) ústavu/katedry	podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Studentka bere na vědomí, že je povinna vypracovat bakalářskou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v bakalářské práci.

. _____ Datum převzetí zadání

_____ Podpis studentky

KOLAŘÍKOVÁ, KRISTÝNA. *Kyberbezpečnost – rizika komunikace na síti*. Praha: ČVUT 2024. Bakalářská práce. České vysoké učení technické v Praze, Masarykův ústav vyšších studií.

MASARYKŮV ÚSTAV
VYŠŠÍCH STUDIÍ
ČVUT V PRAZE

Prohlášení

Prohlašuji, že jsem svou bakalářskou práci vypracovala samostatně. Dále prohlašuji, že jsem všechny použité zdroje správně a úplně citovala a uvádím je v přiloženém seznamu použité literatury.

Nemám závažný důvod proti zpřístupňování této závěrečné práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

V Praze dne: Podpis:

Poděkování

Tímto bych chtěla v první řadě poděkovat Ing. Petru Svobodovi Ph.D., ING.PAEG.IGIP za ochotu, odborné vedení, cenné rady a pomoc při vypracování mé bakalářské práce.

Dále mé poděkování patří rodině za podporu a kolegům u Policie České republiky za odborné rady a pomoc.

Abstrakt

Tématem bakalářské práce je kybernetická bezpečnost a rizika komunikace na síti. V teoretické části jsou popsány hlavní zásady zajištění ochrany informací, pravidla pro bezpečné používání prostředků výpočetní informační techniky a také jednotlivá rizika na síti. Jedním z hlavních témat teoretické části je i vzdělávání v oblasti kybernetické bezpečnosti a její prevence. V praktické části pomocí dotazníkového šetření a rozhovorů autorka zjišťuje úroveň informovanosti a bezpečnosti na síti mezi veřejností vedoucí ke zlepšení vzdělávání uživatelů již od dětství a následné prevenci kybernetické kriminality.

Klíčová slova

Kyberprostor, kybernetická bezpečnost, internet, prevence, vzdělávání, informační a komunikační technologie, kyberšikana, rizika, útočník, oběť

Abstract

The topic of the bachelor's thesis is cybersecurity and the risks of communication on the network. The theoretical part describes the main principles of information protection, rules for the safe use of computing information technology, and various network risks. One of the main topics of the theoretical part is also education in the field of cybersecurity and its prevention. In the practical part, through questionnaires and interviews, the author investigates the level of awareness and security on the network among the public, aiming to improve user education from childhood and subsequently prevent cybercrime.

Keywords

Cyberspace, cybersecurity, internet, prevention, education, information and communication technology, cyberbullying, risks, attacker, victim

Obsah

Úvod a cíl práce

Zvolené téma pro bakalářskou práci “Kyberbezpečnost – rizika komunikace na síti” je v současné době jedním z nejdiskutovanějších témat v oblasti informačních technologií a digitální komunikace. S rozvojem internetu a moderních technologií se zvyšuje množství dat přenášených po síti, což s sebou přináší nejen mnoho výhod, ale i řadu potenciálních rizik. Tato bakalářská práce se zaměřuje na rizika spojená s komunikací na síti, která mohou mít závažné důsledky pro všechny uživatele.

Téma kyberbezpečnosti je dnes aktuálnější než kdy dříve, protože s rostoucí digitalizací každodenního života roste i potřeba osvěty v zabezpečení našich digitálních komunikací a informací.

Teoretická část je rozdělena na 3 kapitoly. V první kapitole jsou vysvětleny základní pojmy, které je potřeba znát pro pochopení celé problematiky kybernetické bezpečnosti. Těmito pojmy jsou kyberprostor, kybernetická bezpečnost a zásady pro její zajištění a sociální sítě. Posledním pojmem této kapitoly je kybernetická trestná činnost, kde jsou vymezeny nejčastější trestné činy spojené s kybernetickými útoky a hrozbami.

Druhá kapitola se pak zabývá jednotlivými kybernetickými hrozbami a útoky, jako jsou spam, hoax, phishing, spear phishing, SIM swap, reverzní inzertní podvody, kyberšikana, kybergrooming, kyberstalking, fake news a hrozby za pomocí umělé inteligence.

Třetí kapitolou je prevence a vzdělávání v kybernetické bezpečnosti. Tato kapitola se zaměřuje na tři nejdůležitější zdroje informací pro každého z nás, a to rodinu, školství a Policii České republiky. Vzdělávání je popsáno jako proces řízeného učení, který je klíčový pro rozvoj společnosti. V kontextu kybernetické bezpečnosti je zdůrazněna nutnost informovat děti o bezpečném používání technologií už od útlého věku. Důležitou roli hraje rodina, která by měla dětem vysvětlovat základy kybernetické bezpečnosti, používat rodičovskou kontrolu a udržovat otevřený dialog o online aktivitách.

Školství také hraje klíčovou roli v prevenci rizikového chování a kyberšikany, kde školy realizují preventivní programy a aktivity za podpory metodických doporučení ministerstva školství. Školní metodici prevence koordinují tyto programy a školí pedagogické pracovníky. Pedagogové mají za úkol sledovat rizikové chování a spolupracovat na vytváření bezpečného školního prostředí.

Policie České republiky provádí preventivní přednášky a projekty zaměřené na různé cílové skupiny, včetně žáků, studentů, rodičů a seniorů, s cílem zvýšit povědomí o kybernetických hrozbách. Policie také spolupracuje na národních a mezinárodních projektech zaměřených na prevenci kyberkriminality.

V poslední řadě třetí kapitola představuje několik preventivních projektů a organizací, které se zaměřují na vzdělávání a prevenci kybernetické bezpečnosti, jako jsou E-Bezpečí, Buď safe online, Internetem Bezpečně, Národní ústav pro kybernetickou a informační bezpečnost, Linka bezpečí, Dětské krizové centrum a Bílý kruh bezpečí. Tyto organizace poskytují vzdělávací materiály, přednášky, kurzy a krizovou pomoc zaměřenou na ochranu před kybernetickými hrozbami.

V praktické části se práce zaměřila na výzkum mezi rodiči, učiteli a policisty, který se skládá ze dvou částí: dotazníkové šetření o povědomí a zkušenostech s kybernetickými útoky a následné rozhovory s vybranými policisty, učiteli a rodiči o prevenci a vzdělávání v oblasti kybernetické bezpečnosti. Výzkumný problém se soustředí na aktuální téma kybernetické bezpečnosti a potřebu aktivního řešení rizik spojených s používáním informačních a komunikačních technologií a internetu. Cílem výzkumu je na základě zjištění o bezpečnostních rizicích a negativních zkušenostech uživatelů přinést nové poznatky pro prevenci a vzdělávání v kybernetické bezpečnosti, s předpokladem, že lepší prevence a vzdělávání povede ke snížení počtu obětí kybernetických útoků.

Ke zpracování bakalářské práce byla použita odborná literatura, ověřené internetové zdroje a některé z platných zákonů. Všechny zdroje byly citovány pomocí webové stránky www.citace.com.

TEORETICKÁ ČÁST

1. Základní pojmy

V této kapitole jsou vysvětleny základní pojmy objevující se v této bakalářské práci, a to kybernetická bezpečnost, kyberprostor, sociální sítě, kybernetická trestná činnost. Vymezení těchto pojmů je důležité k pochopení problematiky této práce.

1.1. Kyberprostor

Než se dostaneme k dalším pojmům jako kybernetická bezpečnost, kybernetická trestná činnost a následně i kybernetickým hrozbám a útokům je důležité si vymezit prostředí, ve kterém se vše odehrává. Tomuto prostředí se odborně říká kyberprostor.

Mezi odborníky není jednotná definice pro kyberprostor. První vysvětlení kyberprostoru z roku 1984 v románu Neuromancer od autora Williama Gibsona je "*Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky… Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v neprostoru mysli, shluky a souhvězdí dat. Jako světla města, …"* [1]

Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti definuje kyberprostor tak, že je "*kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací"*[2].

Na základě těchto informací lze kyberprostor charakterizovat jako digitální prostředí, které my známe jako internet. Obsahuje však také intranet (vnitřní sítě využívané například u Policie ČR a dalších firem a organizací), cloudová úložiště a další služby. Tento digitální prostor je promítnut do našeho světa pomocí informačních a komunikačních technologií (také digitální technologie), jako je například počítač, chytrý mobilní telefon aj. Znaky kyberprostoru jsou globálnost (objevuje se po celém světě),

[1] KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 9788088168317.
[2] §2 písm. a) zák. č. 181/2014 Sb. Zákon o kybernetické bezpečnosti

otevřenost, bohatost na informace a interaktivnost. [3] Důležitou roli zde pak hrají jednotliví uživatelé, kteří mohou ovlivňovat bezpečnost v tomto prostoru.

1.2. Kybernetická bezpečnost

V dnešní době si již život bez informačních a komunikačních technologií (také digitální technologie) nedokáže mnoho lidí představit. Této "závislosti" má ale bohužel hodně osob potřebu zneužívat k obohacení sebe sama. Z toho důvodu je potřeba, aby si každý uživatel digitálních technologií uvědomil, že kybernetická bezpečnost se týká všech a jsou všichni zároveň klíčovým prvkem této bezpečnosti.

Kybernetická bezpečnost je tedy soubor opatření, která musí být přijata, aby byl ochráněn počítačový systém, další prvky informačních a komunikačních technologií, aplikace, data a uživatelé před neoprávněným přístupem nebo útokem, ale také před kriminálním nebo neautorizovaným užitím elektronických dat.[4]

V této práci se autorka zaměřuje zejména na bezpečnost sítí a kybernetická rizika u jednotlivců. Dnešní lidé žijí dva životy ve dvou světech. Jeden je ten fyzický, kde dělají své každodenní aktivity, a druhý svět je ten digitální. O oba tyto světy je potřeba se nějakým způsobem starat, a to hlavně o bezpečnost v nich. V tom fyzickém světě má každý člověk prvky bezpečnosti od mládí zakořeněné, protože k nim byl veden (když odejde z bytu, zamkne dveře, anebo když přechází ulici, tak se rozhlédne). V digitálním světě je to ale mnohem komplikovanější, protože jsou zde mnohem větší rizika a je tu větší pravděpodobnost se s nebezpečím setkat. Proto by si měl každý uživatel informačních a komunikačních technologií uvědomit, že i v tom digitálním světě by se měl chovat co nejbezpečněji.

Zásady zajištění kybernetické bezpečnosti

Cílem kybernetické bezpečnosti je zajistit integritu, důvěrnost a dostupnost informací. K udržení kybernetické bezpečnosti je potřeba dodržování určitých taktik a prvků včetně:

- Bezpečnostní školení zaměstnanců: Vzdělávání zaměstnanců o rizicích a metodách prevence

[3] KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 9788088168317.
[4] KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 9788088168317.

- Aplikace bezpečnostního softwaru a hardware: Použití firewallů, antivirových programů a dalších zabezpečovacích nástrojů
- Pravidelné aktualizace softwaru: Udržování softwaru a operačních systémů aktualizovaných pro redukci zranitelností
- Zálohování dat: Pravidelné zálohování důležitých dat pro případ útoku nebo selhání systému
- Šifrování: Používání šifrování pro ochranu citlivých informací
- Fyzická bezpečnost: Ochrana fyzických míst a zařízení před neoprávněným přístupem
- Ochrana identity a přístupová správa: Omezení přístupu k informacím na nezbytné osoby a monitorování přístupu
- Správa přístupových údajů a citlivých informací, vícefaktorová autentizace[5]

1.3. Sociální sítě

Položme si otázku, kdo v dnešní době nezná sociální sítě? Sociální sítě můžeme 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"*[6]*.*

Nejčastější použití je pomocí chytrých telefonů, kde mohou uživatelé prohlížet a okamžitě reagovat na příspěvky ostatních uživatelů, komunikovat s nimi nebo mít možnost zachycení aktuálního dění v okolí uživatele a rovnou i sdílení. Nejpoužívanější sociální sítě jsou pro uživatele zdarma.

Sociální sítě přináší uživatelům mnoho výhod v reálném životě, avšak mají i rizika. Ty jsou většinou způsobeny malou obezřetností uživatelů, kdy sdílí své osobní údaje a příliš mnoho informací o svém soukromí. Při špatném zabezpečení svého profilu pak mohou být tyto informace zneužity k páchání trestné činnosti.

[5] *10 principů kybernetické bezpečnosti v oblasti ochrany soukromí.* Online. Metodický portál RVP. 2022. Dostupné z: https://spomocnik.rvp.cz/clanek/23385/10-PRINCIPU-KYBERNETICKE-BEZPECNOSTI-V-OBLASTI-OCHRANY-SOUKROMI.html?nahled=. [cit. 2024-05-31].
[6] *Sociální sítě*. Online. Internetem bezpečně. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/socialni-media/socialni-site/. [cit. 2024-06-11].

Mezi nejpoužívanější sociální sítě patří:

- Facebook – jedná se o komplexní a tím i nejpoužívanější sociální síť, která nabízí uživatelům sdílení svých příspěvků, fotek, videí a dále také seznamování a obchodování. Uživatelé zde mohou vytvářet skupiny pro další uživatele se stejným zájmem nebo stránky firem a organizací. Důležitou funkcí je zde chatovací aplikace Messenger, pomocí kterého mohou uživatelé mezi sebou komunikovat. [7]
- Instagram – tato sociální síť slouží především ke sdílení fotografií a videí, kde uživatelé mohou sledovat jak běžné uživatele ale i známé osobnosti. Je zde také možnost komunikace s uživateli[8]
- YouTube – jedná se o sociální síť, kde si uživatelé mohou prohlížet videa, nebo je i sami nahrávat. [9]
- WhatsApp – nejdůležitější funkcí této sociální sítě je rozhodně komunikace s ostatními uživateli. Protože je zde potřeba pro registraci zadat své telefonní číslo, je zde i možnost bezplatně komunikovat pomocí hovoru s uživateli a nově i sdílení aktualit, které jsou viditelné pouze 24 hodin. [10]
- Snapchat – tato sociální síť slouží také ke komunikaci pomocí tzv. “snapů”, kdy si uživatelé zasílají fotografie nebo videa, která se koncovým uživatelům zobrazí jen 1-10 sekund (podle nastavení uživatele) a poté zmizí. [11]
- Tinder – jedná se o sociální síť, která slouží k seznamování uživatelů. Seznámení probíhá tak, že si uživatel vybírá z profilů ostatních uživatelů a ty přijímá nebo odmítá. Při shodě svou přijetí mohou tito uživatelé spolu komunikovat. [12]

1.4. Kybernetická trestná činnost

K rozepsání tohoto tématu využila autorka konzultací s policistou ze Služby kriminální policie a vyšetřování a také vlastních zkušeností z dosavadní již 7 - mi leté praxe ze služby u Policie ČR. V této kapitole je vysvětlena motivace pachatelů ke kybernetické kriminalitě a popsány jednotlivé trestné činy podle zákona č. 40/2009 Sb., trestní zákoník, které mohou být spjaty s kybernetickými útoky.

[7] *Facebook*. Online. Dostupné z: https://www.facebook.com/. [cit. 2024-06-10].
[8] *Instagram*. Online. Dostupné z: https://www.instagram.com/. [cit. 2024-06-10].
[9] *YouTube*. Online. Dostupné z: https://www.youtube.com/. [cit. 2024-06-10].
[10] *WhatsApp*. Online. Dostupné z: https://www.whatsapp.com/. [cit. 2024-06-10].
[11] *Snapchat*. Online. Dostupné z: https://www.snapchat.com/. [cit. 2024-06-10].
[12] *Tinder*. Online. Dostupné z: https://tinder.com/. [cit. 2024-06-10].

Dle dostupných údajů od Policie ČR je kybernetická trestná činnost fenoménem, kterému je věnována stále větší pozornost. Tato trestná činnost je páchaná v kyberprostoru a předmětem útoku jsou informační a komunikační technologie. [13] "*Kriminalita páchaná v kyberprostoru v roce 2023 stále tvoří 10,8 % celkové registrované kriminality. Dle statistických dat je tento trend setrvale stoupající (meziročně +0,6 %, +1 038 skutků)"*[14]

Motivace pachatelů kybernetické kriminality může být různá. Jeden z motivů může být snaha kompenzovat svou nespokojenost s osobním životem. Někteří páchají trestnou činnost za účelem získání moci či výsadního postavení, nebo jen pro pocit převahy (nad veřejností, zaměstnavatelem, policií) a pocit beztrestnosti a neodhalitelnosti. Může se zde objevovat i politický motiv. Nejčastější motiv však bývá obohacení se finančně. [15]

Podvodná jednání

Podle informací autorky přímo od Policie ČR jsou nejčastějšími trestnými činy spáchaných v kyberprostoru:

§209 Podvod

§230 Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací

§234 Neoprávněné opatření, padělání a pozměnění platebního prostředku. [16]

"Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou"[17] se dopouští podvodu. Hlavní motivací tohoto trestného činu v kyberprostoru je získání finančních prostředků. Setkáváme se s ním nejvíce v kybernetickém útoku zvaném Phishing (více v kapitole 2.3.).

[13] *Kyberkriminalita*. Online. Policie České republiky. 2024 Https://www.policie.cz/clanek/kyberkriminalita.aspx. C2024. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx. [cit. 2024-06-16].
[14] *Vývoj registrované kriminality v roce 2023*. Online. Policie České republiky. 2024. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2023.aspx. [cit. 2024-06-16].
[15] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. ISBN 978-80-7380-501-2.
[16] Dle zákona č. 40/2009 Sb. Trestní zákoník
[17] § 209 zákona č. 40/2009 Sb. Trestní zákoník

S tím je úzce spjat trestný čin Neoprávněný přístup k počítačovému systému (…), který je v trestním zákoníku definován jako: *"Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části. Kdo zasáhne do počítačového systému nebo nosiče informací tím, že*

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,

b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,

c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo

d) neoprávněně vloží nebo přenese data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítačového systému nebo jiného technického zařízení pro zpracování dat"[18].

"Kdo sobě nebo jinému bez souhlasu oprávněného uživatele opatří, zpřístupní, přijme nebo přechovává platební prostředek, který umožňuje výběr hotovosti nebo převod peněžních prostředků anebo virtuálních aktiv používaných namísto peněžních prostředků (dále jen "platební prostředek") a který náleží jinému" [19] se pak dopouští neoprávněného zneužití platebního prostředku. Útočník reverzních inzertních podvodů (více v kapitole 2.6.) má právě za cílem opatřit si přístup k platebního prostředku a následně ho zneužít pro svůj prospěch.

Nebezpečné pronásledování

Trestného činu nebezpečné pronásledování se dopouští ten, *"kdo jiného dlouhodobě pronásleduje tím, že*

a) vyhrožuje ublížením na zdraví nebo jinou újmou jemu nebo jeho osobám blízkým,

b) vyhledává jeho osobní blízkost nebo jej sleduje,

[18] §230 zákona č. 40/2009 Sb. Trestní zákoník
[19] §234 zákona č. 40/2009 Sb. Trestní zákoník

c) vytrvale jej prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje,

d) omezuje jej v jeho obvyklém způsobu života, nebo

e) zneužije jeho osobních údajů za účelem získání osobního nebo jiného kontaktu,

a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých"[20].

K tomuto pronásledování tíhnou převážně pachatelé kyberstalkingu (viz kapitola 2.7.). Pronásledování oběti pomocí informačních a komunikačních technologií se pachatelům velmi zjednodušila. Díky možnosti mít veřejný profil na sociálních sítích jdou oběti lehce kontaktovat a pachatel si tak může zajistit informace jako jsou například bydliště, místo studia nebo zaměstnání apod. Je zde využita i výhoda anonymity stalkera, které může využít například k pomluvě nebo vyhrožování.

Pornografie a trestné činy proti dětem

Trestného činu šíření pornografie se dopouští ten, *"kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, v němž se projevuje násilí či neúcta k člověku, nebo které popisuje, zobrazuje nebo jinak znázorňuje pohlavní styk se zvířetem* (..)." Anebo *"kdo písemné, fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo nabízí, přenechává nebo zpřístupňuje dítěti, nebo na místě, které je dětem přístupné, vystavuje nebo jinak zpřístupňuje"*[21].

Položme si však otázku, zda je internet dostatečně zabezpečený v případě používání dětmi. Ano, při vstupu na stránky, kde se nachází pro nezletilé nevhodný obsah, na uživatele vyskočí upozornění o minimální hranici věku. Avšak při kliknutí na tlačítko "souhlasím" už má uživatel plný přístup k obsahu a jiné ověření věku již není potřeba.

Spojením pornografie a dětí se věnují *§192 Výroba a jiné nakládání s dětskou pornografií* a *§193 Zneužití dítěte k výrobě pornografie*[22]. S těmito trestnými činy se můžete setkat v kybergroomingu (viz kapitola 2.8.). Pachatelé se těchto trestných činů dopustí tak, že vylákají z dětí intimní fotky pro

[20] §354 zákona č. 40/2009 Sb. Trestní zákoník
[21] §191 zákona č. 40/2009 Sb. Trestní zákoník
[22] Dle zákona č. 40/2009 Sb. Trestní zákoník

svou potřebu, nebo jich pak využijí k vyhrožování. Při videohovorech si mohou nahrát obrazový záznam dítěte. Cíleně pak i s nabídkou finančního obnosu mohou dítě přimět k výrobě takového obsahu.

Pokud útočník navrhne setkání se sexuálním motivem se pak dopouští trestného činu dle §193b *Navazování nedovolených kontaktů s dítětem*[23].

[23] Dle zákona č. 40/2009 Sb. Trestní zákoník

2. Kybernetické hrozby a útoky

Kybernetickou hrozbu můžeme definovat jako škodlivý pokus o narušení nebo poškození počítačového systému nebo sítě. Tyto pokusy směřují ke změně, krádeži nebo zničení informace, aplikací nebo celého systému. [24] Hrozby mohou mít za zdroj různé technické chyby, ale mohou být také způsobené člověkem, a to jak úmyslně, tak i z nedbalosti. Cílem kybernetické hrozby bývá většinou krádež dat uložených v počítačových systémech, hardware nebo přístupových údajů.

Kybernetický útok od hrozby lze odlišit tím, že kybernetický útok je úmyslné jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby. [25] Útočníkovi jde v takovém útoku o krádež peněz nebo dat, případně zničení nebo odhalení těchto dat. Může se zde jednat o jednání, jako jsou drobné krádeže až po války. Takové útoky mohou směřovat až k poškození, narušení nebo zničení různých podniků.

2.1. Spam

Spam je masově rozesílaná pošta nebo jiná forma komunikace, která je zasílána s komerčními, reklamními nebo podvodnými účely. *"Spam je jeden z nejstarších útoků v kyberprostoru. Dochází zde k distribuci nevyžádané pošty a tím se snaží cílit útok na mobilní zařízení*."[26] Nejčastěji se jedná o e-maily, SMS zprávy, ale mohou se vyskytovat i na sociálních sítích, v komentářích na webových stránkách nebo v diskusních fórech. Hlavním znakem je nevyžádanost a hromadnost. Cílem takového útoku může být propagace produktů, služeb, ale i snaha získat osobní údaje a finanční prostředky z obětí.

[24] KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 9788088168317.

[25] KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 9788088168317.

[26] SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

2.2. Hoax

Hoax je zpráva, jejímž hlavním účelem je šířit paniku. Je zde snaha, aby se příjemce zprávy vyděsil a tím činil unáhlená nebo iracionální rozhodnutí. Nejčastějším obsahem těchto zpráv je právě hrozící nebezpečí nebo zneužití aktuálního dění ve světě a šíření nepravdivých informací. Hoaxem však může být i prosba o pomoc, smyšlené petice, ale také například vtipné zprávy (tzv. novinářské "kachny"). [27],[28] Důvody šíření hoaxů můžou být finanční (on-line podvody), ale i politické a sociální.

2.3. Phishing

Phishing je typ kybernetického útoku, jehož cílem je získat od nic netušících uživatelů citlivé údaje, jako jsou hesla, čísla kreditních karet, údaje o bankovních účtech a další citlivé informace. Útočníci často používají falešné e-maily, SMS zprávy nebo webové stránky, které napodobují důvěryhodné zdroje, jako jsou banky, sociální sítě nebo vládní instituce.

Cílem phishingu je přimět oběť, aby poskytla své citlivé údaje, a přesvědčit ji, že je to nutné z nějakého závažného důvodu, například kvůli potřebě ověřit svůj účet, aktualizovat své údaje nebo se vyhnout zrušení účtu. Oběti v domnění, že komunikují s důvěryhodnou institucí, často poskytnou požadované informace, aniž by si uvědomily, že je ve skutečnosti poskytují podvodníkům.

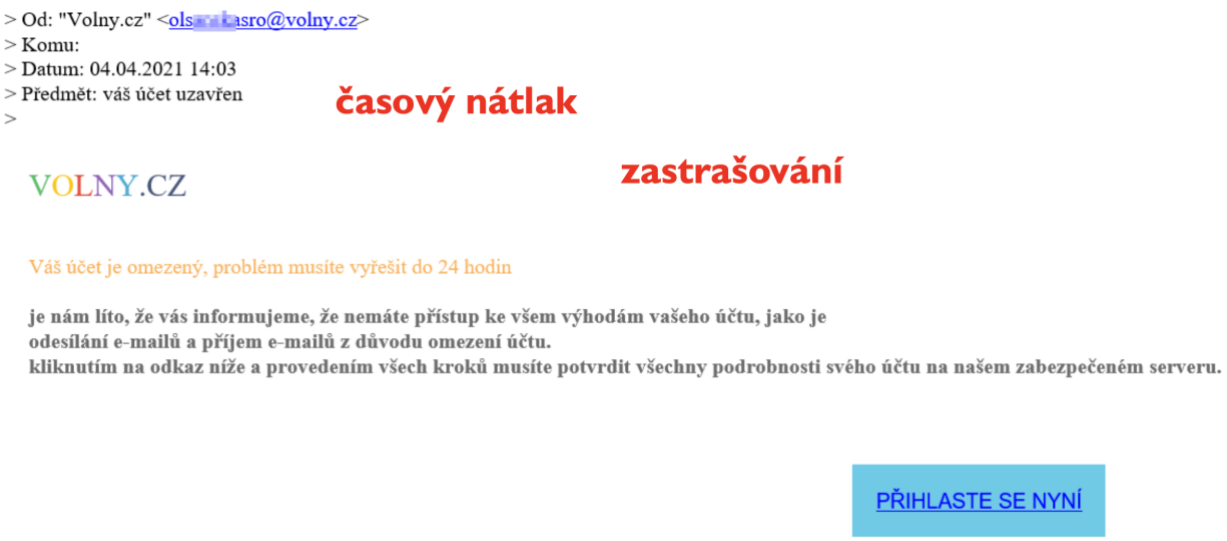
Poddruhy phishingu jsou vishing a smishing. U vishingu místo emailu pachatel používá telefonní číslo a hovorem předstírá existující instituci (např. Energetické společnosti, banky apod.). Smishing je zasílání škodlivých zpráv pomocí SMS a je tím nebezpečnější než phishing – na rozdíl od emailové stránky se SMS netřídí do spamů a zvědavost oběti donutí otevřít podvodný obsah.

Metody phishingu se neustále zdokonalují a útočníci používají stále sofistikovanější techniky, aby bylo obtížné jejich útoky odhalit. Patří mezi ně například používání šifrovaných připojení (https) na falešných webových stránkách, které mohou uživatele uvést v omyl, že stránky jsou zabezpečené. Je

[27] KOPECKÝ, Kamil. *Co je to vlastně ten hoax, dezinformace, misinformace nebo třeba fake news? Čím se tyto termíny liší a co mají společného?* In: E-Bezpečí [online]. 2022 [cit. 2024-04-01]. Dostupné z: https://www.e-bezpeci.cz/index.php/clanky-komentare/2864-co-je-to-vlastne-ten-hoax-dezinformace-misinformace-nebo-treba-fake-news-cim-se-tyto-terminy-lisi-a-co-maji-spolecneho

[28] *Hoax - úvod do problematiky*. In: Policie České republiky [online]. [cit. 2024-04-01]. Dostupné z: https://www.policie.cz/soubor/08-hoax-pdf.aspx

důležité být ostražitý a kriticky posuzovat každou žádost o důvěrné údaje, i když se zdá, že pochází z důvěryhodného zdroje. [29]



Obrázek č.1 – Phishing (zdroj: interní prezentace pro Policii ČR, KAPR, Ondřej. *Podvodná jednání v kybernetickém prostoru z pohledu Policie ČR: Cy3er days.* 2022.)

2.4. Spear phishing

Spear phishing je personalizovaná forma phishingu, která cílí na určitou osobu nebo skupinu osob. Útočníci zde cílí své podvodné e-maily na zaměstnance organizací, u kterých se snaží o krádež dat. Aby byl takový útok úspěšný, musí útočník co nejlépe identifikovat zvolenou osobu. Tato věrohodnost podvodných e-mailů nevzbuzuje v oběti pochybnosti a ta postupuje podle instrukcí. Jednou z forem tohoto útoku může být i podvodných telefonát (vishing), kde se útočník vydává za pracovníka stejné firmy nebo organizace. Pod věrohodným příběhem, že je útočník například pracovník z technické podpory, tak může získat například přihlašovací údaje do systému organizace. [30]

[29] *Phishing*. Online. Internetem bezpečně. 2018. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/podvodne-praktiky/phishing/. [cit. 2024-06-06].
[30] *PODVODNÉ E-MAILY NEBO ZPRÁVY NA SOCIÁLNÍCH SÍTÍCH NA MÍRU: SPEAR-PHISHING A JAK SE PŘED NÍM CHRÁNIT.* Online. NÚKIB. 2020. Dostupné z: https://www.govcert.cz/download/doporuceni/Spear-Phishing.pdf. [cit. 2024-05-27].

2.5. SIM Swap

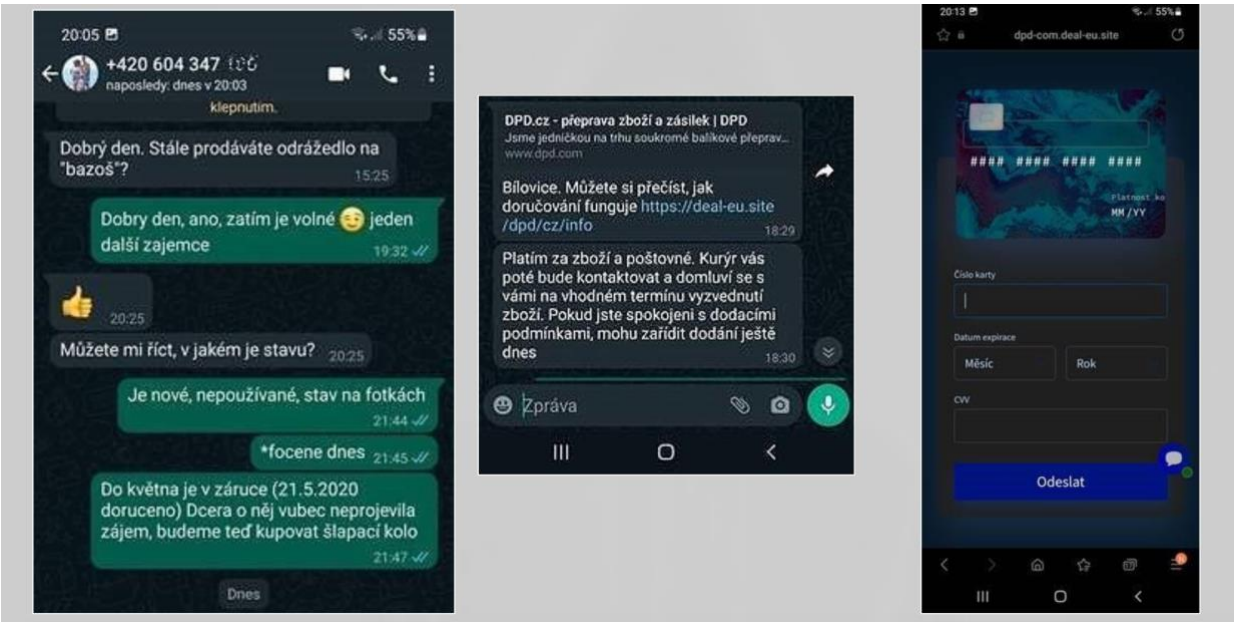
Pachatel se zde vydává za mobilního operátora a donutí oběť si stáhnout jejich mobilní aplikaci za účelem správy služeb. Cíl tohoto útoku je převzetí telefonního čísla pomocí E-sim a zablokování fyzické sim karty. Díky vlastnictví E-sim může mít útočník přístup k dalším účtům oběti a může je dál zneužívat k podvodům. [31]

2.6. Reverzní inzertní podvody

Pachatelé v těchto případech nejprve kontaktují prodávajícího a předstírají zájem o koupi zboží, které nabízí k prodeji. Následuje nabídka zajištění veškerého komfortu spojeného s přepravou a platbou zboží. Poté "kupující" odešle prostřednictvím e-mailu nebo chatovací aplikace fiktivní odkaz zpravidla na přepravní společnost. Jakmile si tento link prodávající otevře, je přesměrován na podvrženou platební bránu, kam vyplní ve většině případů veškeré přihlašovací údaje k elektronickému bankovnictví, platební údaje a rovněž údaje k platební kartě. Bohužel si v této chvíli neuvědomí, že se jedná o podvod. Při kontrole svého bankovního účtu posléze prodejci zjistí, že jim nebyla připsána suma z prodeje zboží, ale naopak byly z účtu finanční prostředky odčerpány. [32]

[31] *Pozor na SIM Swap: nový podvod s appkou mobilního operátora*. Online. Vše o kybernetické bezpečnosti. 2023. Dostupné z: https://cyberblog.cz/mobilni-zarizeni/pozor-na-sim-swap-novy-podvod-s-appkou-mobilniho-operatora/. [cit. 2024-06-11]

[32] *Buďte obezřetní na internetových inzertních portálech*. Online. Policie České republiky. 2022. Dostupné z: https://www.policie.cz/clanek/budte-obezretni-na-internetovych-inzertnich-portalech.aspx. [cit. 2024-05-31].



Obrázek č.2 – Reverzní inzertní podvod (zdroj: interní prezentace pro Policii ČR, KAPR, Ondřej. *Podvodná jednání v kybernetickém prostoru z pohledu Policie ČR: Cy3er days.* 2022.)

2.7. Kyberstalking

Kyberstalking představuje využití internetu nebo jiných elektronických prostředků k pronásledování nebo obtěžování jednotlivce, skupiny či organizace. Může zahrnovat nepravdivá obvinění, pomluvy, urážky na cti a pomluvy. Dále může zahrnovat monitorování, krádež identity, vyhrožování, vandalismus, nabídky sexu nebo vydírání. Toto chování způsobuje narušení digitálního života jednotlivce, stejně jako negativně ovlivňuje mentální a emoční pohodu oběti a její pocit bezpečí. Kyberstalking je často provázen reálným stalkingem. Stalker může být cizí osoba nebo někdo, koho oběť zná. Pro stalkera je však výhodná anonymita. [33]

"Kyberstalking jsou *opakované a dlouhodobé pokusy kontaktovat oběť pomocí dopisů, e-mailů, telefonátů, SMS zpráv, zasíláním různých zásilek s dárky, zasíláním vzkazů na ICQ, Skype, různé druhy chatu, VoIP apod. Obsah těchto zpráv může být příjemný až veselý, ale též urážející, zastrašující. Výjimkou nejsou zprávy původně příjemné, snažící se získat odpověď či kontakt oběti, až později po*

[33] *Kyberstalking*. Online. Internetem Bezpečně. 2018. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyberstalking/. [cit. 2024-06-11].

zprávy urážející, nevkusné či zastrašující. V rámci snahy kontaktovat oběť je využívána široká paleta citů (vyhrožování, vydírání, vyvolávání pocitu viny apod.).” [34]

V rámci prevence proti kyberstalkingu je důležité zajistit přísná bezpečnostní nastavení osobních účtů, být opatrný ohledně sdílení osobních informací na internetu a hlásit jakékoliv obtěžování na konkrétní sociální síti, kde se odehrává, a v případě potřeby kontaktovat Policii ČR.

2.8. Kybergrooming

Kybergrooming je proces "přátelství" s mladou osobou s cílem o online sexuální kontakt a/nebo osobní setkání s ní za účelem páchání sexuálního zneužití. Hlavními cíli kybergroomingu jsou získat důvěru dítěte, získat intimní a osobní údaje od dítěte (často sexuální povahy, jako jsou sexuální rozhovory, obrázky nebo videa) za účelem vyhrožování a vydírání. Pachatelé často přijímají falešné identity dítěte nebo dospívajícího a oslovují své oběti na webových stránkách přívětivých k dětem, čímž děti zůstávají zranitelné a bez povědomí o tom, že byly kontaktovány za účelem kybergroomingu. Pachatelé často začínají konverzaci nevinnými a obecnými otázkami o věku, zálibách, škole, rodině a také lákají děti na dárky. Po získání důvěry často požadují, aby dítě sdílelo nahé fotky nebo videa a zapojilo se do sexuálně zneužívajících konverzací. Mnozí z nich také cíleně pozvou dítě na osobní schůzku. Anonymita a dostupnost digitálních technologií umožňují groomerům oslovit více dětí najednou, čímž se exponenciálně násobí případy. Prevence a ochrana zahrnují opatření, jako je vyhýbání se interakci s cizími lidmi přes internet, nesdílení soukromých a důvěrných informací, pravidelná kontrola nastavení soukromí na webových stránkách a sociálních sítích, neakceptování dárků nebo nabídek od cizích lidí, blokování a nahlášení každého, kdo se pokouší o online zneužívání, a sdělení rodičům, opatrovníkům nebo důvěryhodným dospělým o jakýchkoli špatných zkušenostech v online prostředí. [35]

O tomto druhu útoku byl natočen a vydán v roce 2020 dokumentární film s názvem *V síti* z režie Víta Klusáka a Barbory Chalupové. Jsou zde obsazeny 3 dospělé herečky s vizáží nezletilých dívek a ty

[34] *Co je to stalking a cyberstalking*. Online. E-Bezpečí. C2008-2023, s. 1. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kyberstalking/66-23. [cit. 2024-04-01].

[35] KOPECKÝ, Kamil; SZOTKOWSKI, René a DOBEŠOVÁ, Pavla. *Riziková komunikace a seznamování českých dětí v kyberprostoru*. Online. Olomouc: Univerzita Palackého v Olomouci, 2021. ISBN 978–80–244–5915–8. Dostupné z: https://e-bezpeci.cz/index.php/ke-stazeni/odborne-studie/146-rizikova-komunikace-a-seznamovani-ceskych-deti-v-kyberprostoru-2021/file. [cit. 2024-04-01].

se nachází ve svých pokojích, které jsou vytvořeny v ateliérech. Živě je zde zachycena komunikace s útočníky, kteří si herečky v přestrojení sami vyhledali na sociálních sítích a naplňují zde veškeré znaky tohoto útoku přes snahu získání důvěry obětí, vyžadování intimních fotografií, sexu přes videohovory, zasílání odkazů na porno nebo fotografií svých intimních partií s následným vyhrožováním a snahou vylákat oběť na schůzku. Tvůrci tohoto dokumentárního filmu zároveň vytvořili webové stránky, kde se věnují tzv. Osvětové kampani. Na těchto webových stránkách se nachází spousta videí a postupů prevence a řešení své pozice v rámci kybergroomingu (dítě, rodič, učitel nebo predátor). [36]

2.9. Kyberšikana

Kyberšikana se odehrává prostřednictvím informačních a komunikačních technologií, jako jsou mobilní telefony, počítače a tablety. Může probíhat prostřednictvím SMS, textových zpráv, nebo online na sociálních médiích, kde lidé mohou zobrazovat a sdílet obsah.

"Kyberšikana je kolektivní označení forem šikany prostřednictvím elektronických médií, jako je internet a mobilní telefony, které slouží k agresivnímu a záměrnému poškození uživatele těchto médií. Stejně jako tradiční šikana zahrnuje i kyberšikana opakované chování a nepoměr sil mezi agresorem a obětí." [37]

Kyberšikana zahrnuje odesílání, zveřejňování nebo sdílení negativního, škodlivého, nepravdivého nebo zlomyslného obsahu o někom jiném. Může také zahrnovat sdílení osobních nebo soukromých informací o někom jiném, čímž způsobuje rozpaky nebo ponížení. Některé formy kyberšikany mohou překročit hranici do nezákonného nebo trestného chování. [38]

Nejčastější místa, kde dochází ke kyberšikaně, zahrnují sociální sítě, jako jsou Facebook, Instagram, Snapchat a TikTok, textové zprávy a zprávy v aplikacích na mobilních telefonech nebo tabletech, online chaty přes internet, online fóra, chatovací místnosti a diskusní skupiny a online herní komunity.

[36] *Osvětová kampaň V síti.* Online. V síti. 2020. Dostupné z: https://vsitifilm.cz/. [cit. 2024-06-06].
[37] Priceová a Dalgleish in Černá, Dědková a kol., 2013 str. 20
[38] *Co je kyberšikana?* Online. E-Bezpečí. C2008-2023. Dostupné z: https://www.e-bezpeci.cz/index.php/kontakt/71-trivium/1418-co-je-kybersikana. [cit. 2024-06-11].

2.10. Fake News

Za fake news se považují nepravdivé zprávy, ale i média, která tyto zprávy tvoří. Tyto média se snaží o větší sledovanost tím, že zveřejní polopravdy nebo nepravdivé informace jak o politicích, celebritách ale snaží se opírat i o aktuální dění a okolnosti přikreslovat. [39] Dochází zde k misinformacím a dezinformacím. Příkladem jednoho z největších témat, kolem kterého bylo nejvíc fake news, byla určitě pandemie koronaviru. Docházelo k šířením různých konspiračních teorií i vzniku a šíření infekce, ale také o způsobech zjištění infekce a její léčby a důvodech smrti.

2.11. Umělá inteligence

Umělá inteligence je již nějakou dobu součástí našeho života. Umělá inteligence je počítačová věda, která se zabývá schopností strojů napodobovat lidské schopnosti. Důležitá je zde i schopnost z dostupných dat se učit a trénovat své zkušenosti, a to za pomocí neuronových sítí. Objevuje se například v podobě pomocníků do domácnosti (robotické vysavače, chytří asistenti), aplikací generujících různý nový obsah a má velký potenciál do budoucna v rámci lékařství, bezpečnosti a dalších odvětví, které by měly společnosti pomoci ulehčit život. [40]

Umělá inteligence může být však užitečná i různým podvodníkům a pachatelům trestné činnosti. Nabízí se zde možnost vytvořit podvodná telefonní čísla k voláním lidem za účelem obohacení se. Umělá inteligence umí i věrně napodobit hlas známé osobnosti a také pomocí fotek vytvořit video. Díky takovým videím může docházet k takzvaném Deep Fake. Jedná se o realistické úpravy videí a rozpohybování fotografií známých osobností a tím dochází k šíření dezinformací v on-line prostředí. Zde je velice riskantní rychlé učení v úpravě videí, a tak i čím dál horší rozeznávání autenticity videí. [41] Díky takové schopnosti umělé inteligence vznikají například i podvodné investiční reklamy. Útočník zde využije tvář známé osobnosti, vytvoří z jeho hlasu nahrávku a láká na výhodné investice do známých institucí. Aby takové video bylo účinnější, mohou si útočníci zaplatit reklamu, aby taková "lákavá"

[39] KOPECKÝ, Kamil. *FAKE NEWS - ÚVOD DO PROBLEMATIKY.* E-Bezpečí 2017, 2(2): Page 34-39. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=1264
[40] KOPECKÝ, Kamil. *Umělá inteligence.* Online. In: YouTube. 2023. Dostupné z: https://youtu.be/OCdHMXxl3fk?si=9Igh9wFTNvJpw_pE. [cit. 2024-05-19].
[41] KOPECKÝ, Kamil. *Deep fake - stručný úvod do problematiky.* E-Bezpečí, roč. 4, č. 1, s. 23-25. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=1417

nabídka proběhla na co nejvíce sociálních sítích nebo platformách, jako je například YouTube. Oběť, která je například fanouškem zneužité tváře osobnosti, tak otevře odkazující stránku a zasílá peníze s vidinou výhodné investice, která se však investorovi nikdy nevrátí.

3. Vzdělávání a prevence v oblasti kybernetické bezpečnosti

Prevence kriminality " *zahrnuje soubor nerepresivních opatření, tedy veškeré aktivity vyvíjené státními, veřejnoprávními i soukromoprávními subjekty směřující k předcházení páchání kriminality a snižování obav z ní. Patří sem opatření, jejichž cílem či důsledkem je zmenšování rozsahu a závažnosti kriminality a jejích následků, ať již prostřednictvím omezení kriminogenních příležitostí, nebo působením na potenciální pachatele a oběti trestných činů. Jedná se o opatření sociální prevence, situační prevence, včetně informování veřejnosti o možnostech ochrany před trestnou činností a pomoci obětem trestných činů.*"[42]

Vzdělávání můžeme definovat jako "*proces řízeného učení a vyučování, k němuž dochází typicky v edukačním prostředí školy nebo v jiném edukačním prostředí (…). Jedna z forem vzdělávání je také individuální sebevzdělávání. Z hlediska společnosti je vzdělávání jednou z nezbytných podmínek jejího přežití a vývoje."*[43]

Děti a mládež dnešní doby se do prostředí počítačů, chytrých telefonů a dalších zařízení již narodila. Autorka si troufne tvrdit, že drtivá většina si už každodenní život bez těchto zařízení a zejména internetu nedokáže představit. Děti využívají internet zejména z důvodu komunikace a hraní her, avšak to může být jednoduše spojeno i s riziky kybernetických hrozeb a útoků. Z toho důvodu by mělo probíhat informování dětí hned od začátku používání informačních a komunikačních technologií a internetu o tom, jak by se měly chovat bezpečně při jejich používání. Informovanost by měla započít hlavně ze strany rodiny, poté školství a také následně od dalších institucí.

3.1. Rodina

Rodina je pro dítě zdrojem opory a podpory. O pouto rodič-dítě by se mělo pečovat v reálném životě, ale i v on-line prostředí. Taková "on-line" výchova dítěte by měla probíhat od samého začátku,

[42] *Prevence kriminality.* Online. Ministerstvo vnitra České republiky. 2024. Dostupné z: https://www.mvcr.cz/clanek/web-o-nas-prevence-prevence-kriminality.aspx?q=Y2hudW09MQ%3D%3D. [cit. 2024-06-11].
[43] PRŮCHA, Jan a VETEŠKA, Jaroslav. *Andragogický slovník*. Praha: Grada, 2012. ISBN 978-80-247-3960-1.

kdy začne dítě používat informační a komunikační technologie, a měla by se přizpůsobovat věku dítěte. Rodič by měl svému dítěti vysvětlovat, jak si má počínat, aby bylo v bezpečí a nevystavilo se zbytečně hrozbám na internetu. Zde jsou základní body a doporučení, kterých by se měl každý rodič držet:

- Vysvětlení dětem základů kybernetické bezpečnosti, jako je důležitost silných hesel, ochrana osobních údajů a nebezpečí spojené se sdílením příliš mnoha informací on-line. Je důležité, aby děti zjistili, proč je důležité sdílet informace pouze s lidmi, které zná dítě osobně.
- Používání rodičovské kontroly na zařízeních a v aplikacích, aby bylo možné sledovat a omezovat přístup k nevhodném obsahu. Zároveň je vhodné nastavení filtrů, které blokují rizikové webové stránky
- Udržování rozhovoru s dětmi o jejich aktivitě on-line a utvoření bezpečného a důvěrného prostředí pro hlášení nepříjemných situací, do kterých se dítě může v on-line prostoru dostat
- Vzdělávání zábavnou formou – na internetu je množství videí, které mohou dětem vysvětlit, jak se hrozbám a útokům ubránit, ale také jak jim předcházet
- Rodiče jako příklad – děti se nejlépe učí napodobováním, a rodiče jsou pro ně ten nejlepší vzor hned od raného věku. Rodič by tedy měl sám dodržovat zásady kybernetické bezpečnosti. [44]

Je důležité, aby dítě mělo svého průvodce světem on-line. Rodič by měl mít sám přehled o kybernetické bezpečnosti, aby tak své zkušenosti a znalosti mohl předávat svým dětem. Jak se má dítě chovat v on-line prostoru, zjistit, co je vhodné a co nevhodné sdílet na sociálních sítích, jak se má chovat k neznámým lidem v on-line prostředí ale i v reálném životě je velice důležité pro udržení jeho bezpečí.[45]

3.2. Školství

Pedagogika je vědní disciplína zabývající se teorií a praxí výchovy a vzdělávání. Studuje procesy, metody a techniky, které slouží k rozvoji osobnosti jedince ve všech jeho aspektech – intelektuálním, sociálním, emocionálním i fyzickém. Pedagogika se zaměřuje na vytváření a analýzu vzdělávacích programů, výzkum efektivity různých výchovných přístupů a metod, a také na otázky morálního a

[44] *Desatero dobrého "kybernetického" rodiče.* Online. Internetem bezpečně. 2018. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rodice/desatero-dobreho-kybernetickeho-rodice/. [cit. 2024-05-31].
[45] ŠEVČÍKOVÁ, Anna. *Děti a dospívající online: vybraná rizika používání internetu.* Psyché (Grada). Praha: Grada, 2014. ISBN 978-80-247-5010-1.

etického rozvoje jedinců. Cílem pedagogiky je optimalizovat vzdělávací procesy tak, aby co nejlépe podporovaly osobní růst a společenský rozvoj. [46]

Vzdělávání ve školách je proces systematického předávání znalostí, dovedností, hodnot a postojů prostřednictvím formálního školského systému. Tento proces je organizován a řízen učiteli a institucemi a probíhá v rámci strukturovaného kurikula. Cílem školního vzdělávání je rozvíjet intelektuální, sociální, emocionální a fyzické schopnosti studentů, aby byli připraveni na život a práci ve společnosti. Vzdělávání ve školách zahrnuje různé úrovně, od předškolního vzdělávání přes základní a střední školu až po vyšší odborné a vysokoškolské studium. [47]

Primární prevence rizikového chování u dětí, žáků a studentů na školách je opřena o metodické doporučení Ministerstva školství, mládeže a tělovýchovy České republiky. Tato prevence se zaměřuje na agresi, šikanu, závislostní chování, sexuální rizikové chování ale i kyberšikanu a další rizikové formy komunikace v kyberprostoru. Tato metodická doporučení jsou určené pro školy a školské zařízení zřízené ministerstvem školství a pomáhají školám předcházet a eliminovat rizikové projevy chování u svých žáků a studentů.

V rámci metodického doporučení a organizace primární prevence je zde důležitá osoba, a to **školní metodik prevence**, který má na starosti tyto činnosti:

Metodické a koordinační činnosti:

- Koordinuje tvorbu a dohlíží na realizaci preventivního programu školy.
- Organizuje a podílí se na aktivitách školy zaměřených na prevenci záškoláctví, závislostí, násilí, vandalismu, sexuálního zneužívání, sekt, kriminality, sebepoškozování a dalších sociálně patologických jevů.
- Metodicky vede pedagogické pracovníky v oblasti prevence sociálně patologických jevů, jako je identifikace problémového chování a preventivní práce s třídními kolektivy.
- Koordinuje vzdělávání pedagogických pracovníků v oblasti prevence.
- Organizuje aktivity zaměřené na integraci multikulturních prvků do vzdělávacího procesu a prevenci rasismu a xenofobie.
- Koordinuje spolupráci školy s orgány státní správy, samosprávy, poradnami a odbornými pracovišti v oblasti prevence sociálně patologických jevů.

[46] ŠAFRÁNKOVÁ, Dagmar. *Pedagogika*. 2. Grada Publishing, 2019. ISBN 978-80-271-1190-9.
[47] JANÍK, Tomáš a PEŠKOVÁ, Karolína. *Školní vzdělávání: podmínky, kurikulum, aktéři, procesy, výsledky.* Online. Brno: Masarykova univerzita, 2013. ISBN 978-80-210-6396-9. Dostupné z: https://munispace.muni.cz/library/catalog/view/7/3454/1008-1/1#preview. [cit. 2024-06-01].

- V případě výskytu sociálně patologických jevů kontaktuje odborná pracoviště a podílí se na intervenci a následné péči.
- Shromažďuje odborné zprávy a informace o žácích v poradenské péči, s ohledem na ochranu osobních údajů.
- Vede písemné záznamy o činnosti, opatřeních a realizovaných aktivitách v oblasti prevence.

Informační činnosti:

- Zajišťuje a předává odborné informace o sociálně patologických jevech, preventivních programech a metodách primární prevence pedagogickým pracovníkům.
- Prezentuje výsledky preventivní práce školy a získává nové odborné informace a zkušenosti.
- Vede a aktualizuje databázi spolupracovníků školy v oblasti prevence (orgány státní správy a samosprávy, střediska výchovné péče, poradny, zdravotnická zařízení, Policie ČR, orgány sociální péče, nestátní organizace, krizová centra a další).

Poradenské činnosti:

- Vyhledává a provádí orientační šetření u žáků s rizikem či projevy sociálně patologického chování; poskytuje poradenské služby těmto žákům a jejich zákonným zástupcům a zajišťuje péči odborných pracovišť ve spolupráci s třídními učiteli.
- Spolupracuje s třídními učiteli při zachycování varovných signálů sociálně patologických jevů a sleduje úroveň rizikových faktorů ve škole.
- Připravuje podmínky pro integraci žáků se specifickými poruchami chování a koordinuje poskytování poradenských a preventivních služeb těmto žákům ve spolupráci se specializovanými školskými zařízeními.

Dalšími důležitými osobami ve školním prostředí v rámci prevence jsou třídní učitelé a další pedagogičtí pracovníci. Ti mají na starost spolupráci se školním metodikem prevence a snaží se zachytit varovné signály, získávají a udržují si přehled o osobních zvláštnostech žáků a také o jejich rodinném zázemí. Motivují také k dodržování školního řádu, nastavování pravidel a jejich dodržování ve třídách a podporují pozitivní a bezpečnou atmosféru v třídních kolektivech. [48]

[48] *Metodické doporučení k primární prevenci rizikového chování u dětí, žáků a studentů ve školách a školských zařízeních.* Online. Ministerstvo školství, mládeže a tělovýchovy České republiky. 2010. Dostupné z: https://msmt.gov.cz/uploads/Metodicke_doporuceni_uvodni_cast.doc. [cit. 2024-06-02].

Z rozhovoru školitele a koordinátora projektu *Safer internet Centrum Česká republika* Martina Kožíška se dozvídáme, že v oblasti kybernetické bezpečnosti je úrověň znalostí mezi žáky a studenty poměrně dobrá. Avšak domnívá se, že se školy zaměřují na nesprávná témata kybernetické bezpečnosti. Bylo by ideální obohatit formu předávání informací z přednášek a filmů o workshopy, peer-2-peer programy z důvodu, aby děti samy chtěly předávat své zkušenosti směrem k učitelům, mezi sebou ale i rodičům.[49] Školy se při nedostatečné informovanosti v problematice mohou obracet na Policii České republiky a případně i další projekty zaměřující se na šíření osvěty v kybernetické bezpečnosti jako například projekt Buď safe online, který stvořila společnost Avast za spolupráce s youtuberem Jiřím Králem.[50]

3.3. Policie České republiky

"Policie České republiky je jednotný ozbrojený bezpečnostní sbor." [51] Jedná se o jeden z nejpočetnějších bezpečnostních sborů v České republice. "*Jejím úkolem je chránit bezpečnost osob a majetku a veřejný pořádek, předcházet trestné činnosti, plnit úkoly podle trestního řádu a další úkoly na úseku vnitřního pořádku a bezpečnosti svěřené jí zákony* (..)."[52]

U české policie slouží k roku 2024 kolem 40000 příslušníků. [53] Policisté jsou přiřazení na různé útvary. Tyto útvary jsou Policejní prezidium České republiky, útvary policie s celostátní působností, krajská ředitelství policie (celkem 14) a útvary zřízené v rámci těchto ředitelství. Celá Policie České republiky je podřízena ministerstvu vnitra.

Každé ze 14 krajských ředitelství policie má své oddělení prevence, které se zaměřuje na nejaktuálnější problematiky trestné činnosti. Oddělení prevence "*provádí v rámci své působnosti činnost po linii prevence na metodické, kontrolní i výkonné úrovni směrem k dalším součástem policie,*

[49] *Nebezpečí číhá na síti. O kyberbezpečnosti by se neměli učit jen žáci na školách*. Online. Eduklub. 2024. Dostupné z: https://www.eduklub.cz/2024/01/11/nebezpeci-ciha-na-siti-o-kyberbezpecnosti-by-se-nemeli-ucit-jen-zaci-na-skolach/. [cit. 2024-06-02].
[50] *Víš, jak být na internetu v klidu a v bezpečí?* Online. Buď safe online. 2020. Dostupné z: https://www.avast.com/cz/besafeonline/. [cit. 2024-06-02].
[51] §1 zák.č. 273/2008 Sb. Zákon o Policii České republiky
[52] §2 zák.č. 273/2008 Sb. Zákon o Policii České republiky
[53] *Policie loni přijala 2334 lidí, po dvou letech počet policistů stoupl.* Online. České noviny. 2024, 1.2.2024. Dostupné z: https://www.ceskenoviny.cz/zpravy/2473843. [cit. 2024-06-01].

včetně mezinárodní spolupráce (..)"[54]*.* Hlavním cílem těchto oddělení je činnost směřující ke snížení kriminální činnosti v České republice a tím zvyšování bezpečnosti občanů státu.

Hlavní činnosti v prevenci kybernetické kriminality oddělení prevence realizují v podobě přednášek a projektů pro různé cílové skupiny – žáky a studenty základních a středních škol, učitele, rodiče ale i pro seniory. Ve školním prostředí realizují přednášky na téma Kyberšikana, Bezpečné chování na internetu, Kyberšikana a počítačová kriminalita nebo Trestní odpovědnost. [55]

Vedle těchto preventivních přednášek policie zároveň spolupracuje na různých projektech. Jedním z největších projektů je ve spolupráci s ČSOB "Tvoje cesta onlinem". Tento projekt je postaven na aktivitách cílených na bezpečí v kyberprostoru a zahrnuje metodiky, přednášky a informační kampaně. Policie však v této problematice spolupracuje i na mezinárodních kampaních. Jednou z nich je kampaň Europolu #SayNo!, která se zaměřuje na zneužívání dětí on-line. V České republice vznikla tak podoba této kampaně s veřejně dostupnými preventivními videi od Policie České republiky pod názvem "Řekni ne!". [56]

3.4. Preventivní projekty

V této kapitole autorka představí vybrané projekty a organizace, které se zabývají prevencí kybernetické bezpečnosti:

E-Bezpečí

E-Bezpečí je jeden z největších projektů realizovaný Centrem prevence rizikové virtuální komunikace Pedagogické fakulty univerzity Palackého ve spolupráci s dalšími organizacemi je zaměřený na prevenci, vzdělávání, výzkum, intervenci a osvětu kybernetické bezpečnosti. Specializuje se zejména na:

- *"Kyberšikanu a sexting (různé formy vydírání, vyhrožování, poškozování oběti s pomocí informačních a komunikačních technologií)*

[54] *Odbor prevence.* Online. Policie České republiky. 2024. Dostupné z: https://www.policie.cz/clanek/odbor-prevence.aspx. [cit. 2024-06-01].
[55] *Prevence*. Online. Policie České republiky. 2024. Dostupné z: https://www.policie.cz/clanek/prevence-609977.aspx. [cit. 2024-06-01].
[56] Prevence kyberkriminality. Online. Policie České republiky. 2024. Dostupné z: https://www.policie.cz/clanek/prevence-kyberkriminality.aspx. [cit. 2024-06-01].

- *Kybergrooming (komunikace s neznámými uživateli internetu vedoucí k osobní schůzce)*
- *Kyberstalking a stalking (nebezpečné pronásledování s použitím ICT)*
- *Rizika sociálních sítí (zejména sítě Facebook)*
- *Hoax, spam a fake news*
- *Online závislosti (netolismus, nomofobie)*
- *Youtubering*
- *Zneužití osobních údajů v prostředí elektronických médií."*[57]

Svou činnost projekt provádí pomocí práce s různými cílovými skupinami, a to pomocí přednášek a vzdělávacích akcí, které jsou podloženy skutečnými kauzami. Mezi cílové skupiny patří žáci a studenti, učitelé, preventisté, metodici prevence, policie ale i rodiče. Mezi kapacity v oboru, které na stránkách projektu publikují své články, patří například prof. Mgr. Kamil Kopecký, Ph.D..

Buď safe online

Projekt "*Buď safe online"* je cílený na žáky základních škol a zábavnou formou předává dětem informace o tom, jak se mají chovat bezpečně na internetu. Vznikl za podpory ministerstva školství, mládeže a tělovýchovy České republiky v roce 2018 spoluprací společnosti Avast a influencera a youtubera Jirky Krále, kdy společně zrealizovali přednášky na školách. V roce 2020 byl představen web projektu, kde se nachází interaktivní online kurz, který mohou využívat rodiče i učitelé při své výuce. [58]

Internetem Bezpečně

Zakladatelem projektu je Roman Kohout, který zde využil zkušenosti ze služby u Policie České republiky jako vyšetřovatel kybernetické trestné činnosti. Zabývá se vzdělávacími aktivitami s cílem zvyšovat povědomí o rizicích a hrozbách v online prostředí. Cílovým skupinami jsou žáci a studenti škol, rodiče, učitelé, zaměstnanci OSPOD a další. Projekt realizuje nezisková organizace *you connected, z.s.*.

"Mezi hlavní vzdělávací aktivity projektu patří:

- *provoz webových stránek internetembezpecne.cz*
- *facebooková stránka Internetem Bezpečně*

[57] *Informace o projektu.* Online. E-Bezpečí. 2023. Dostupné z: http://www.e-bezpeci.cz/index.php/o-projektu/oprojektu. [cit. 2024-06-02].
[58] *Buď safe online*. Online. Avast. 2020. Dostupné z: https://www.avast.com/cz/besafeonline/. [cit. 2024-06-02].

- *realizace odborných přednášek pro laickou i odbornou veřejnost*
- *vydávání odborných publikací a dalších podpůrných vzdělávacích materiálů*
- *organizace odborných konferencí."*[59]

Národní ústav pro kybernetickou a informační bezpečnost

"Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany." [60] Tento projekt vznikl na základě změny zákona o kybernetické bezpečnosti.

Na oficiálních stránkách NÚKIB nalezneme rozdělovník, kterým se dostaneme do nabídky online vzdělávacích kurzů v oblasti kybernetické bezpečnosti. Cílovým skupinami jsou zde předškoláci, žáci základních škol a studenti středních škol, pedagogy přes seniory a další veřejnost. Většina kurzů jsou veřejně přístupná, pár jich je však dostupná pouze s certifikátem (např. Kurz pro zaměstnance zdravotnictví nebo pro úředníky územních samosprávních celků).

Linka bezpečí

Linka bezpečí je již od roku 1994 bezplatná pomoc dětem a dospívajícím v krizových situacích ale i při řešení každodenních starostí a problémů. Linka je dostupná telefonicky, chatu nebo prostřednictvím e-mailů nonstop ve formě poradny. Realizují i preventivní akce ve školách, pomocí vzdělávacích videí nebo blogem. Na oficiálních stránkách nalezneme i dostupné články v online poradně, kde jedním z nich je i směřován na bezpečnost v online prostoru. Jsou zde rady, jak předcházet kybernetickým hrozbám, jak poznat útok v kyberprostoru a jak se mu bránit. Jsou zde dostupné i nejčastěji kladené otázky dětí a dospívajících z oblasti sextingu, kybergroomingu nebo kyberšikany. [61]

Dětské krizové centrum

Tato nestátní nezisková organizace byla založena v roce 1992 prof. MUDr. Jiřím Dunovským DrSc. a poskytuje bezplatnou krizovou odbornou pomoc dětem, které jsou týrané, zanedbávané nebo

[59] *O projektu*. Online. Internetem Bezpečně. 2018. Dostupné z: https://www.internetembezpecne.cz/o-projektu/. [cit. 2024-06-02].
[60] *O NÚKIB*. Online. NÚKIB. 2017. Dostupné z: https://nukib.gov.cz/cs/o-nukib/. [cit. 2024-06-02].
[61] *Poradna - Online.* Online. Linka bezpečí. 2024. Dostupné z: https://www.linkabezpeci.cz/poradna/online. [cit. 2024-06-02].

sexuálně zneužívané. Kromě krizové pomoci nabízí Dětské krizové centrum sociálně aktivizační služby a nonstop linku důvěry, kde nalezneme kontakt i na linku specializující se na rizika kyberprostoru. [62]

Bílý kruh bezpečí

Bílý kruh bezpečí je nestátní nezisková organizace založena v roce 1991. Tato organizace nabízí nonstop bezplatnou pomoc obětem a svědkům trestných činů a pozůstalým po obětech. Pomoc poskytují vždy odborníci jako psychologové, sociální pracovníci nebo právníci pomocí linky, intervenčních center, centrály nebo celostátních sítí poraden.

K dalším aktivitám Bílého kruhu bezpečí patří spolupráce při tvorbě zákonů, preventivní činnosti formou přednášek, seminářů, tvorba vlastních projektů a mezinárodní spolupráce. [63]

[62] *O Dětském krizovém centru.* Online. Dětské krizové centrum. 2024. Dostupné z: https://www.ditekrize.cz/o-detskem-krizovem-centru/. [cit. 2024-06-02].
[63] *Poslání a činnost.* Online. Bílý kruh bezpečí. 2024. Dostupné z: https://www.bkb.cz/o-nas/poslani-a-cinnost/. [cit. 2024-06-02].

PRAKTICKÁ ČÁST

4. Výzkumné šetření

V praktické části se autorka zaměřila na výzkumné šetření cílené na rodiče, učitele a policisty. Šetření je rozděleno na dvě části – dotazníkové šetření zaměřující se na povědomí a zkušenost respondentů s kybernetickými útoky s návazností na rozhovory s 2 policisty, 2 učiteli a 2 rodiči o prevenci a vzdělávání v kybernetické bezpečnosti.

Autorka si k získání informací vytvořila dotazník v aplikaci Forms od společnosti Microsoft Office. Dotazník byl složen z 1 otevřené otázky a 13 uzavřených otázek týkajících se tématu bakalářské práce a byla zde možnost výběrových odpovědí s jednou nebo více možnostmi, hodnotící odpovědi nebo s možností vlastní odpovědi. Jednotlivé otázky dotazníku jsou uvedeny v příloze č.1. Zveřejnění dotazníku proběhlo koncem března roku 2024. Autorka dotazník rozeslala pomocí sociálních sítí a zpráv do řad učitelů, policistů a rodičů. Cíl pro počet respondentů byl 105 (každá zastupující skupina po 35 respondentech). Vyhodnocení proběhlo po 1 měsíci sběru odpovědí. Zcela zodpovězených dotazníků bylo 102 a tak byla návratnost z 97 %.

Otázky v rozhovorech byly otevřené a počet otázek byl následující – pro rodiče 9 otevřených otázek, pro učitele 7 otevřených otázek a pro policisty 6 a 7 otevřených otázek. Jednotlivé otázky jsou uvedené v příloze č. 3. Rozhovory proběhly osobně nebo telefonicky koncem května 2024.

Kritéria pro výběr respondentů byla následující:

Rodiče – věk dětí alespoň 6 let a více

Učitelé – učí alespoň 5 let na základní škole, střední škole nebo středním odborném učilišti

Policisté – ve službě policie alespoň 5 let, u rozhovorů bylo potřeba zaměření na kybernetickou kriminalitu a prevenci

4.1. Výzkumný problém, cíl výzkumu

Kybernetická bezpečnost je v současné době velmi aktuální téma. K rizikům, která se mohou objevit při používání informačních a komunikačních technologií a internetu, je potřeba se nějakým způsobem postavit a aktivně je řešit. Jedním z nejdůležitějších řešení je rozhodně prevence ve formě vzdělávání dětí, ale i dalších věkových kategorií uživatelů, o zásadách kybernetické bezpečnosti. Troufám si tvrdit, že čím lepší a obsáhlejší bude v této oblasti prevence a vzdělávání, tím bude menší počet obětí kybernetických útoků a kybernetické kriminality.

Hlavní cíl výzkumného šetření je na základě zjištění, s jakými bezpečnostními riziky se uživatelé setkali a zda mají negativní zkušenost, **přinesení nových poznatků v rámci prevence a vzdělávání v kybernetické bezpečnosti.**

Na základě tohoto cíle byly stanoveny tyto výzkumné otázky:

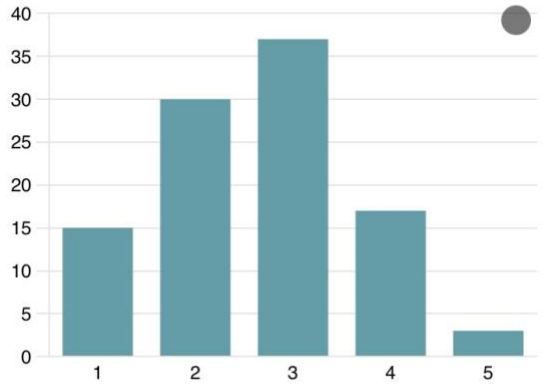
1. **Jak probíhá vzdělávání a prevence v oblasti kybernetické bezpečnosti?**
2. **Jakou mají respondenti zkušenost s kybernetickými útoky?**
3. **Jak setkání s kybernetickým útokem respondenti řešili?**

4.2. Výsledky dotazníkového šetření

1. Jak by jste ohodnotil svou schopnost používat ICT technologie?

Další podrobnosti Přehledy

2.64
Průměrné hodnocení

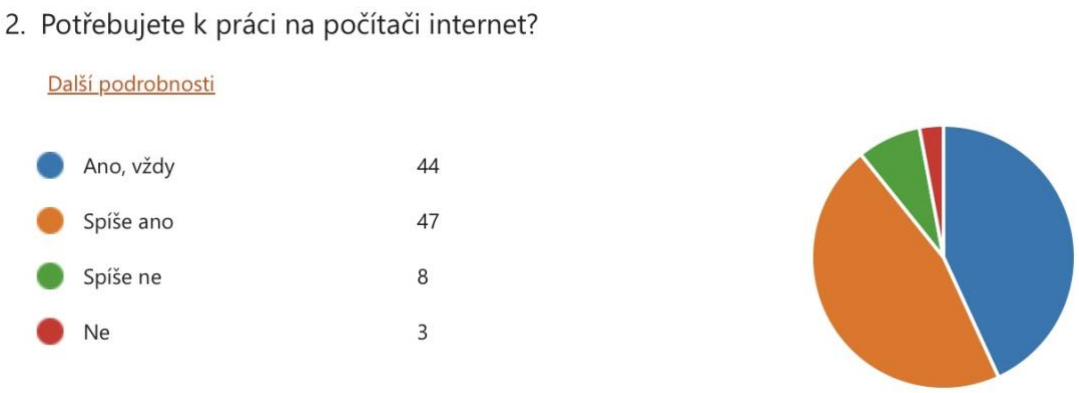


Otázka č.1: **Jak byste ohodnotil svou schopnost používat ICT technologie?**

Graf č.1 - Schopnost používat ICT technologie (zdroj: vlastní výzkum 2024)

První otázka byla založena na sebereflexi respondentů, jak by ohodnotili jako ve škole na stupnici 1-5 svou schopnost používání informačních a komunikačních technologií. Výsledek se zde nejvíce blíží známce 3, což ukazuje spíše na horší schopnost. Vzhledem k věku respondentů, který se nejvíce pohyboval mezi 26-35 lety, se zde může objevit myšlenka, zda se lidé, kteří jsou ve věku více jak 25 let dostatečně vzdělávali v používání informačních a komunikačních technologií. U mladších generací už totiž předpokládáme, že se s technologiemi setkávají čím dál dřív a mají tak v tomto ohledu větší schopnosti a zkušenosti.

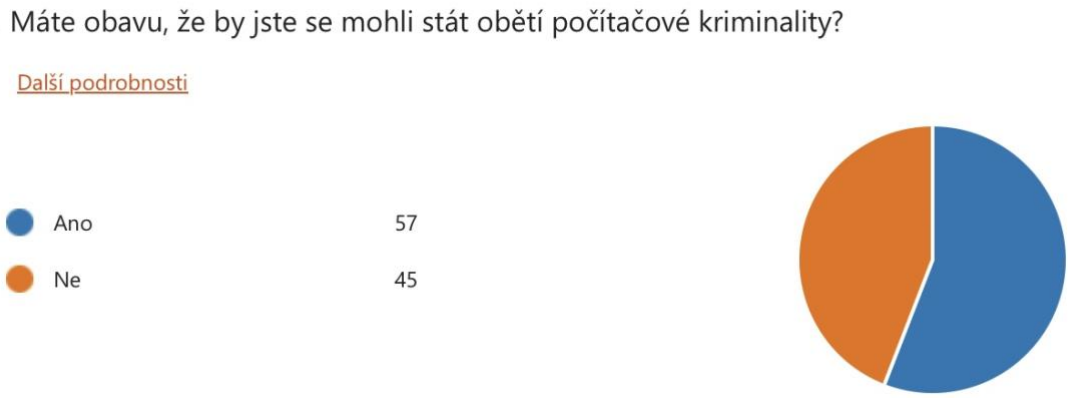
Otázka č.2: **Potřebujete k práci na počítači internet?**



Graf č.2. - Potřeba internetu k práci (zdroj: vlastní výzkum 2024)

Výsledky druhé otázky nám ukazují, že už drtivá většina práce na počítači je postavena na použití internetu.

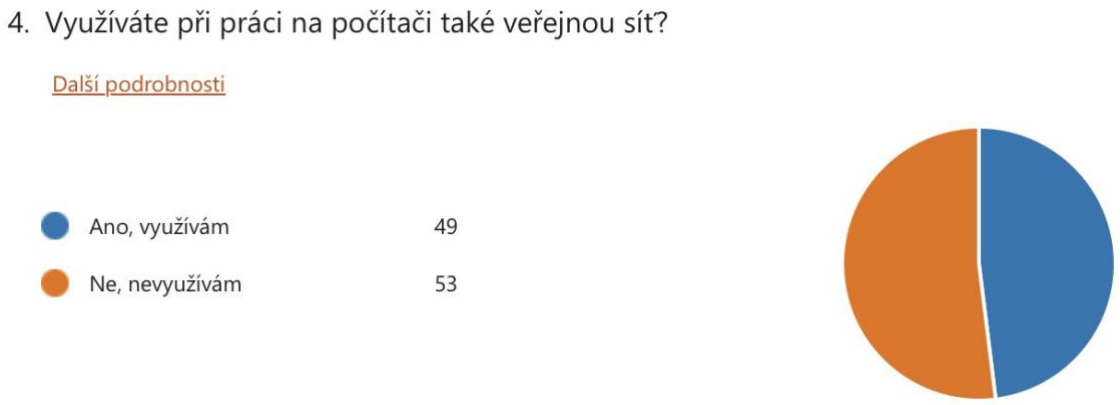
Otázka č.3: **Máte obavu, že byste se mohli stát obětí počítačové kriminality?**



Graf č.3 - Obava z počítačové kriminality (zdroj: vlastní výzkum 2024)

Výsledky třetí otázky ukazují, že větší část respondentů má obavu z možného rizika počítačové kriminality. Tento výsledek naznačuje vysokou úroveň podvědomí o hrozbách v kyberprostoru.

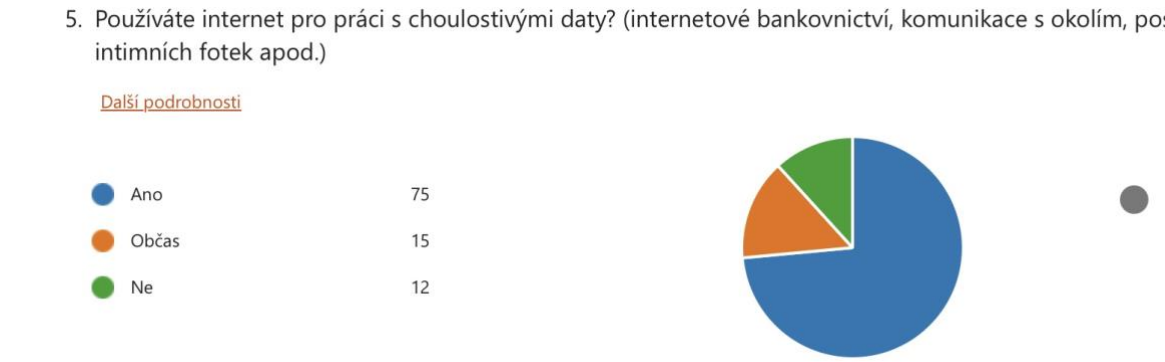
Otázka č.4: **Využíváte při práci na počítači také veřejnou síť?**



Graf č.4 - Využití veřejné sítě (zdroj: vlastní výzkum 2024)

Výsledek 4.otázky znovu ukazuje relativně vysokou úroveň podvědomí respondentů o kybernetických hrozbách, kdy většina z nich nevyužívá veřejnou síť k práci na internetu. Preference soukromé a zabezpečené sítě rozhodně může ovlivnit bezpečnost v kyberprostoru.

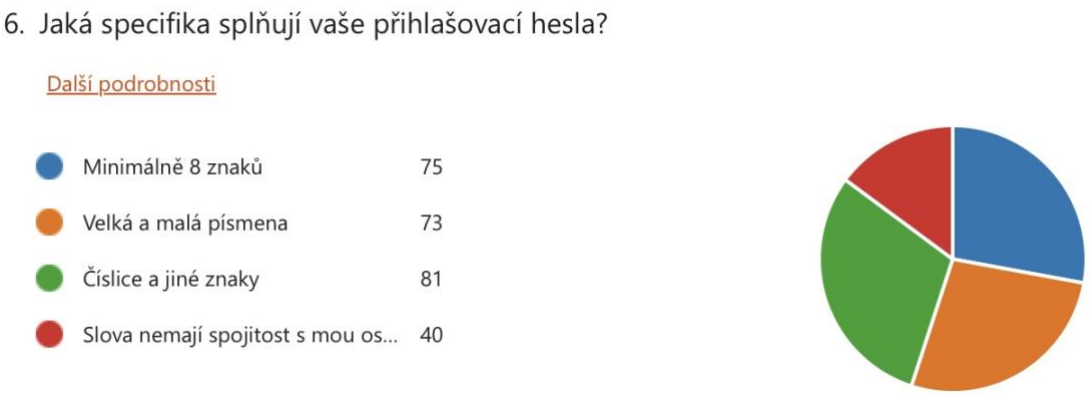
Otázka č.5: **Používáte internet pro práci s choulostivými daty? (Internetové bankovnictví, komunikace s okolím, posílání intimních fotek apod.)**



Graf č.5 - Choulostivá data (zdroj: vlastní výzkum 2024)

Výsledky 5.otázky ukazují, že drtivá většina dotazovaných pravidelně používá internet k práci s choulostivými daty. Tento výsledek naznačuje vysokou míru závislosti na internetu pro důležité a citlivé činnosti mezi respondenty. Bylo by dobré zde zdůraznit, že i v takové situaci je však potřeba myslet na důležitost zabezpečení a ochrany soukromí, aby tato práce s internetem nebyla zneužitelná neoprávněným osobami.

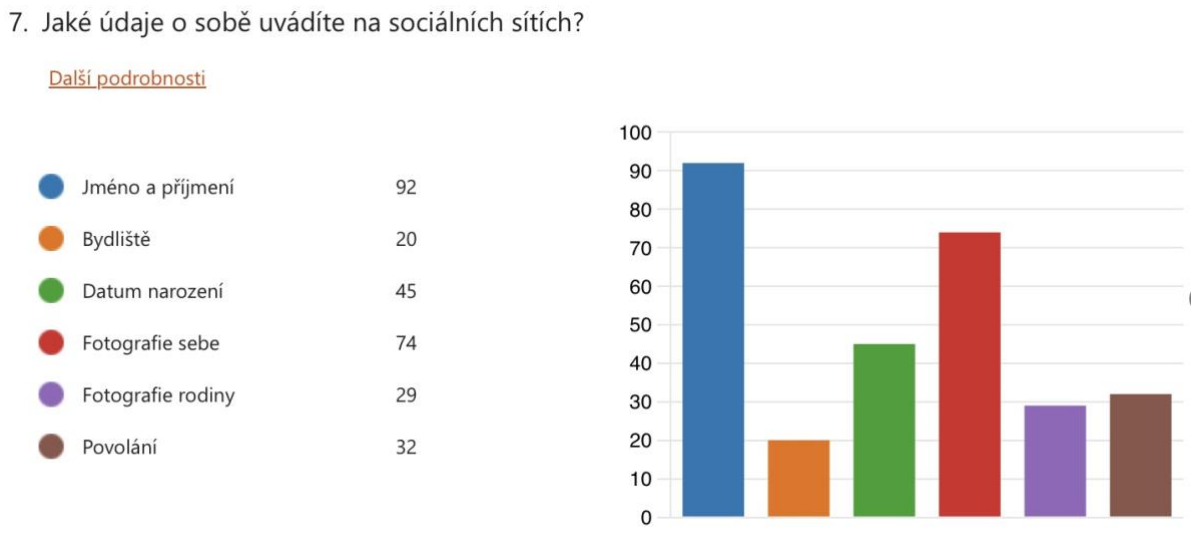
Otázka č.6: **Jaká specifika splňují Vaše přihlašovací hesla?**



Graf č.6 - Specifika hesel (zdroj: vlastní výzkum 2024)

Jedním z důležitých faktorů zabezpečení svých účtů před zneužitím je síla hesla. Jak jsou na tom respondenti se svými hesly ukazují výsledky otázky č.6. Většina respondentů dodržuje dobré praktiky pro vytváření silných hesel, jako je minimální délka, kombinace velkých a malých písmen a zahrnutí číslic a speciálních znaků. Nicméně méně jak polovina respondentů používá v heslech slova, která nemají spojitost s jejich osobou, což je kritický prvek pro zvýšení bezpečnosti. **Celkově jsou respondenti dobře informováni o základních pravidlech tvorby silných hesel, ale je zde stále prostor pro zlepšování.**

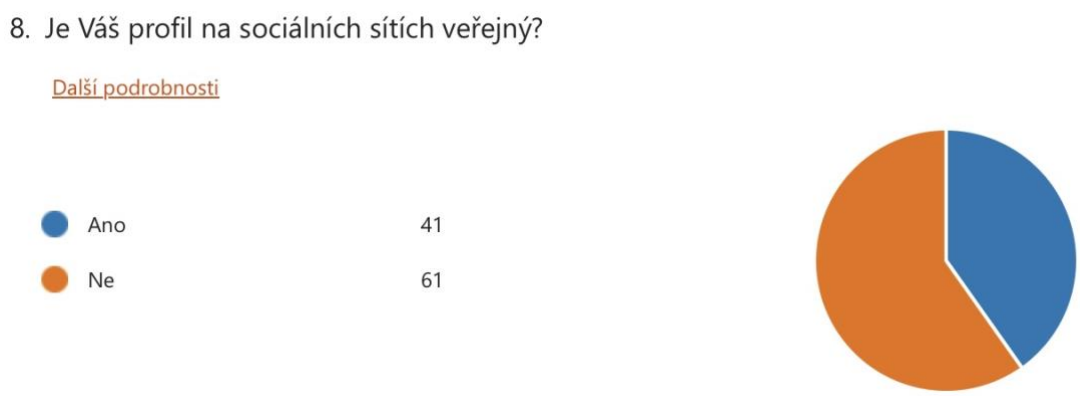
Otázka č.7: **Jaké údaje o sobě uvádíte na sociálních sítích?**



Graf č.7 - Údaje na sociálních sítích (zdroj: vlastní výzkum 2024)

Výsledky 7.otázky ukazují, že většina respondentů sdílí na sociálních sítích základní identifikační údaje, jako jsou jméno, příjmení, datum narození a fotografie sebe. Opatrnější jsou při sdílení citlivějších údajů, jako je bydliště nebo fotografie rodiny, což je velice dobře, protože by mohly vést k rizikům směřujícím jak přímo k nim, tak i k jejich rodinám.

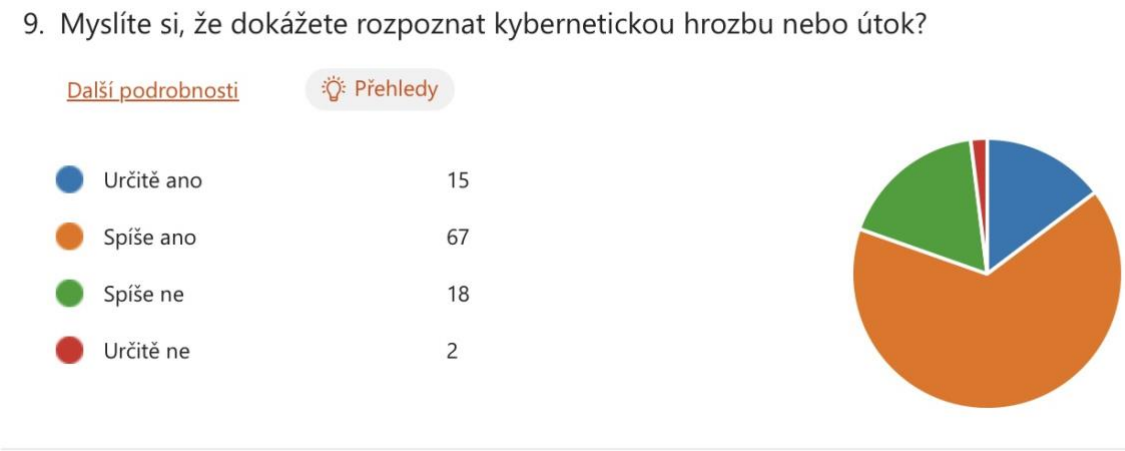
Otázka č.8: **Je Váš profil na sociálních sítích veřejný?**



Graf č.8 - Veřejný profil na sociálních sítích (zdroj: vlastní výzkum 2024)

Na předchozí otázku navazuje otázka č.8. Výsledky této otázky ukazují, že většina respondentů si chrání své soukromí na sociálních sítích tím, že mají své profily nastavené jako soukromé. To znamená, že jejich informace a příspěvky jsou viditelné pouze pro schválené uživatele. Přesto téměř 40 % respondentů má veřejné profily, což vystavuje vyššímu riziku zneužití jejich osobních údajů a obsahu, který sdílejí. Tento výsledek naznačuje, že zatímco většina lidí si uvědomuje potřebu ochrany svého soukromí online, stále existuje významná skupina, která preferuje nebo jí nevadí veřejný přístup k jejich informacím na sociálních sítích.

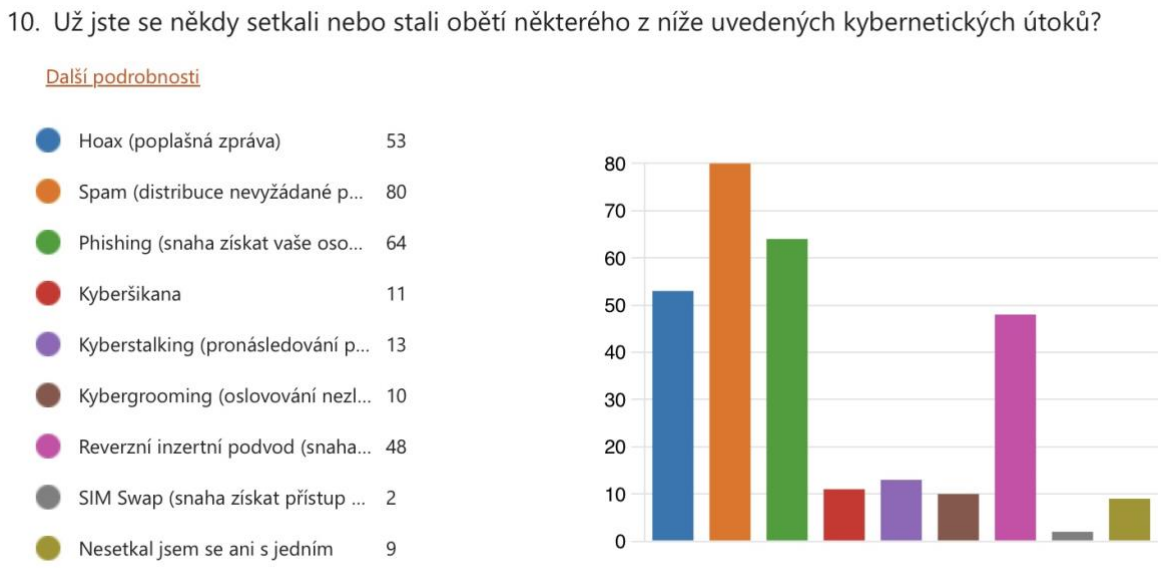
Otázka č.9: **Myslíte si, že dokážete rozpoznat kybernetickou hrozbu nebo útok?**



Graf č.9 - Schopnost rozpoznat kybernetický útok (zdroj: vlastní výzkum 2024)

Výsledky 9.otázky ukazují, že většina respondentů je relativně sebevědomá ve své schopnosti rozpoznat kybernetickou hrozbu nebo útok. Přesto je tu stále dost respondentů, kteří mají pochybnosti nebo si jsou jisti, že nedokážou kybernetickou hrozbu rozpoznat. **Tento výsledek naznačuje, že zatímco většina lidí má alespoň základní důvěru ve své schopnosti rozpoznávání kybernetických hrozeb, stále existuje významná část populace, která by potřebovala další vzdělávání a trénink v oblasti kybernetické bezpečnosti.**

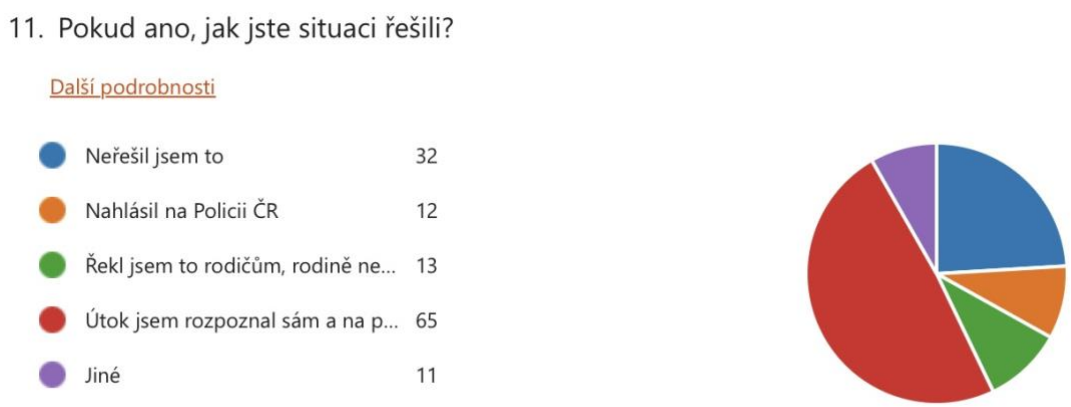
Otázka č.10: **Už jste se někdy setkali nebo stali obětí některého z níže uvedených kybernetických útoků?**



Graf č.10 - Kybernetické útoky (zdroj: vlastní výzkum 2024)

Výsledky 10.otázky ukazují, že respondentů (kromě 9 šťastlivců) má zkušenost s alespoň jedním typem kybernetického útoku, přičemž spam a phishing jsou nečastější. To naznačuje vysoké zkušenosti a povědomí o kybernetických hrozbách mezi respondenty. Přítomnost méně častých, avšak závažných útoků, jako je kyberstalking a kybergrooming, podtrhuje nutnost zvýšené opatrnosti a ochrany soukromí na internetu. **Vzhledem k vysokému počtu respondentů, kteří se setkali s kybernetickými útoky, je důležité pokračovat v osvětě a vzdělávání o kybernetické bezpečnosti.**

Otázka č.11: **Pokud ano, jak jste situaci řešili?**



Graf č.11 - Řešení kybernetických útoků (zdroj: vlastní výzkum 2024)

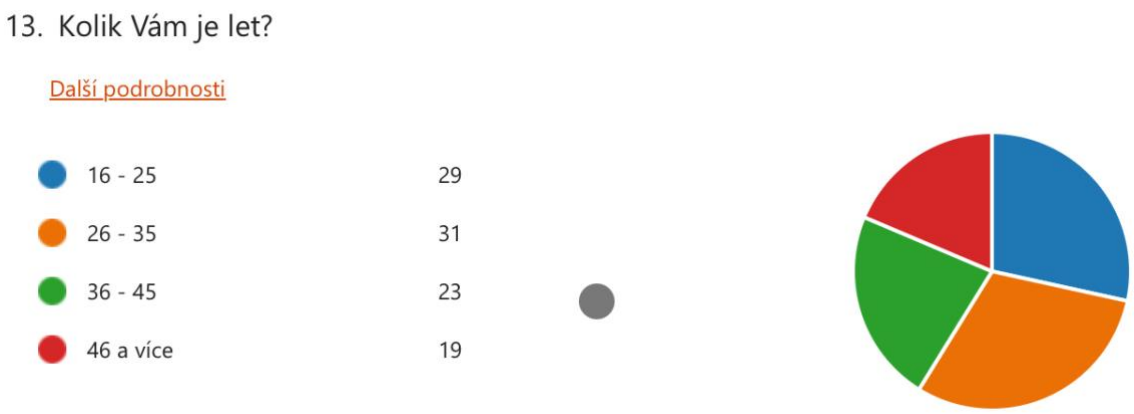
Výsledky 11.otázky navazují na zkušenosti s kybernetickými útoky z předchozí otázky. Vyplývá z toho, že více jak polovina respondentů byla schopna samostatně rozpoznat a zastavit kybernetickými útok, což zase ukazuje na dobré povědomí a schopnosti v oblasti kybernetické bezpečnosti. **Nicméně značný počet respondentů situaci vůbec neřešil, což může naznačovat buď neznalost správných postupů, nebo podceňování závažnosti útoků. Malá část respondentů nahlásila incident na Policii ČR, což naznačuje potřebu většího povědomí o možnostech právní ochrany a také větší snahu o důvěru ze strany policie. Někteří respondenti se obrátili na své blízké, což je také důležitý krok pro zajištění podpory a poradenství. Celkově je zde však prostor pro zlepšování v oblasti informovanosti a reakce na kybernetické útoky.**

Otázka č.12: **Dozvěděli se již v minulosti jak hrozby nebo útoky rozpoznat a jak se bránit? A pokud ano, napište prosím, od koho jste se informace dozvěděli.**

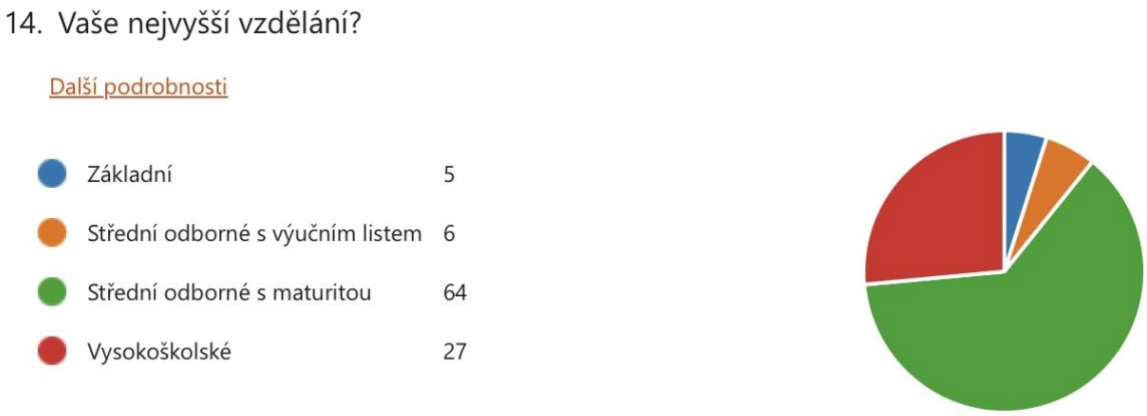
Tato otázka byla pro respondenty otevřená a vzniklo zde mnoho možností odpovědí. Odpovědí Ne zde odpovědělo 24 respondentů. Někteří respondenti odpovědi svou vlastní zkušeností (8). Větší zbytek respondentů 67 odpovědělo Ano a rozepsala se kde k informacím přišli. Nejčastější odpovědi jsou zde škola nebo školení, práce, Policie ČR, internet, banka, rodina nebo známí. Všechny odpovědi na tuto otázku jsou uvedeny v příloze č.2.

Tyto výsledky ukazují, že větší skupina respondentů má nějaké povědomí o tom, jak rozpoznat kybernetické hrozby a jak se proti nim bránit, a to díky různým zdrojům. Přesto téměř čtvrtina respondentů tuto informovanost postrádá, což poukazuje na potřebu dalšího vzdělávání a informování veřejnosti o kybernetických hrozbách a způsobech ochrany. **Důležitým výsledkem je zde však také to, že nejvíce informací o prevenci kybernetické bezpečnosti je ze strany školství, Policie ČR, zaměstnání, internetu a rodiny.**

Otázka č.13: **Kolik Vám je let?**



Graf č.12 - Věk (zdroj: vlastní výzkum 2024)



Otázka č.14: **Vaše nejvyšší vzdělání?**

Graf č.13 - Vzdělání (zdroj: vlastní výzkum 2024)

4.3. Výsledky rozhovorů

RODIČ Č.1

1. **Jaká je Vaše pracovní pozice a náplň Vaší práce?**

   Analytik - zpracování digitálních dat, IT služby.

2. **Jak vnímáte kybernetickou kriminalitu?**

Jako velký problém, který stále sílí s tím, jak roste digitalizace všeho. Využití klasických technik podvodu (časový nátlak, hra „na city“, zaštítění se nějakou „autoritou“, role útočníka jakožto zachránce, …) má možnost v digitálním prostředí oslovit opravdu široké masy potenciálních obětí napříč zeměmi a kontinenty. Naproti tomu snahy o vyšetření podvodů naráží na omezení dané jednotlivými právními prostředími jednotlivých zemí a časové limity pro uchování provozních dat komunikací.

3. **Předpokládám, že jste se už někdy setkal/a s kybernetickým útokem, jak jste se v této situaci zachoval/a?**

Snahy o podvod vůči mé osobě skončily stejně rychle jak začaly. Dokázal jsem je sám poznat a reagovat ideálně blokováním útočníka, aby mě už nemohl kontaktovat.

4. **Účastnil/a, nebo se pravidelně účastníte vzdělávání v problematice kybernetické bezpečnosti? (Např. Školení, kurzy, e-learning apod.)**

   Ano, pravidelně i na mezinárodní úrovni.

5. **Jakým způsobem získané informace předáváte dál? (Děti, dospívající, kolegové a další osoby ve vašem okolí)**

Jedním slovem – „osvěta“. Bohužel ve většině případů je to až ve chvíli, kdy už je pozdě. Kde to jde, tak se snažím informovat, poradit, poskytnout pomoc s nastavením apod., ale nejde úplně všem „na potkání“ zkontrolovat telefon, počítač a dát přednášku o bezpečném pohybu v digitálním prostoru.

6. **Jak staré máte děti?**

   Stáří dětí je do 10 ti let.

7. **Jak často a jak dlouho je necháváte využívat internet? Máte přehled o jejich aktivitě na internetu a sociálních sítích?**

Vlastní telefony ani počítače zatím nemají a pokud si nějaké takové zařízení mohou půjčit, tak v naší domácnosti je pod kontrolou (dítě nebo zařízení). Situace na návštěvách a ve škole je samozřejmě jiná – daleko horší.

8. **Jakým způsobem se je snažíte chránit před kybernetickými hrozbami?**

Zde opět platí aplikování „osvěty“ jen pomalejšími kroky (vzhledem k věku).

9. **Jaká je podle Vás ideální prevence problematiky kybernetické bezpečnosti?**

Informace by měly být předávány od mala – jak rodiči, tak učiteli už od školky. Dále by mělo být v zájmu každého vzdělávat se – věnovat jednou za čas 5 minut nějakému článku nebo tématu (namísto sledování krátkých videí v metru nebo na WC). Dále používat „selský rozum“ a poučku „když nevím, tak se zeptám“ (nebo si to najdu). Téma je to rozsáhlé, ale získání povědomí o základních pojmech či druzích podvodů, je klíčové pro úspěšnou obranu sebe nebo blízkých osob.

RODIČ Č.2

1. **Jaká je Vaše pracovní pozice a náplň Vaší práce?**

Pracuji jako asistent prodeje a provozní vedoucí. Mou náplní práce je obsluha půjčovny a prodejny se sportovním vybavením, rozvrh směn zaměstnanců, objednávky doplnění zboží a odpovědnost za bezproblémový provoz.

2. **Jak vnímáte kybernetickou kriminalitu?**

Kybernetickou kriminalitu vnímám jako velký problém. Ať už se jedná o klamavé nabídky, napadání účtů na sociálních sítích, vydírání, falešné webové stránky, “predátory” na komunikačních platformách či krádeže identit. Často jsou obětmi této formy kriminality děti či senioři, kteří jsou důvěřiví či zkrátka málo informovaní o hrozbách v kybernetickém prostoru.

3. **Předpokládám, že jste se už někdy setkal/a s kybernetickým útokem, jak jste se v této situaci zachoval/a?**

Ano. Bohužel hned několikrát.

Kdybych měla vybrat ty, dle mě nejzásadnější, jednalo by se například o situaci cca před 20 lety. Bylo mi 20 a Pohybovala jsem se na chatovacím kanále "lide.cz". Komunikovala jsem tam s mužem cca ve věku cca 45 let. Nabízel mi práci společnice a vyvíjel nátlak, abych na nabídku kývla. V rámci "vábení" se zmínil, že se nemám čeho bát, že pro něj pracují i 14-15 ti letá děvčata. Toto konstatování mi přišlo alarmující. Kontaktovala jsem polici, že mám podezření na pedofílii a zneužívání nezletilých. Byla jsem pozvána na policejní stanici k podání výpovědi. Dozvěděla jsem se, že daného pána již mají v hledáčku a že má výpověď určitě pomohla vyšetřování.

Další nepříjemná zkušenost se odehrála cca před 3 lety. Byly mi napadeny všechny účty, e-mail, skrz který zařizuji vše důležité od pojištění po internetové bankovnictví. Změnila jsem všechna hesla a druhý den byl účet znovu napaden. Postupně mi začal "kyber útočník" měnit všechna hesla sám a já začala ztrácet přístup. Dokonce mi i přišel e-mail z mého vlastního e-mailu, kde jsem byla informována, že mi byly odcizeny všechny přístupové údaje a pokud nepošlu do konkrétního termínu na jejich účet vysoký obnos peněz, budou všechny jim dostupné informace zveřejněny včetně mých kompromitujících fotografií, které pořídili díky přístupu ke kameře mého mobilního telefonu. Kontaktovala jsem společnost seznam.cz, u které mám e-mail vedený. Za jejich asistence jsme vytvořili velmi silné heslo a a tím hacker již neměl přístup k mým ověřovacím e-mailům a já postupně získala své účty zpět.

4. **Účastnil/a, nebo se pravidelně účastníte vzdělávání v problematice kybernetické bezpečnosti? (Např. Školení, kurzy, e-learning apod.)**

Ničeho obdobného se neúčastním. Nejspíš stále spoléhám na svůj instinkt, vědomosti a IT dovednosti.

5. **Jakým způsobem získané informace předáváte dál? (Děti, dospívající, kolegové a další osoby ve vašem okolí)**

Samozřejmě se o svou zkušenost podělím, pokud na to přijde konverzační téma. Každý den si čtu novinky ze světa a pokud se objeví článek o kyber útoku, přečtu si jej a případně upozorním své okolí. Co se týče bezpečnosti dětí, skvělý krok byl dokument "V SÍTI". To by měl vidět každý rodič.

6. **Jak staré máte děti?**

Mám 2 dcery. 15 a 8 let.

7. **Jak často a jak dlouho je necháváte využívat internet? Máte přehled o jejich aktivitě na internetu a sociálních sítích?**

Přístup na internet výrazně neomezuji. Pokud mají hotové školní povinnosti, mohou trávit svůj čas libovolným způsobem. Nesleduji jejich prohlížecí historii a většinou se se mnou podělí o informace, které jim přijdou důležité.

8. **Jakým způsobem se je snažíte chránit před kybernetickými hrozbami?**

Mluvím s nimi čas od času o potřebné skepsi k informacím, které dostávají, že né každý je tím, za koho se vydává, že schůzky "na slepo" jsou velmi nebezpečné a co vše se může stát, pokud by na takovou schůzku šly a neinformovaly mne. Také jsem jim vysvětlila, jaké fotografie nesdílet ani veřejně ani soukromě po zprávách. To je zatím primárně apel na starší dceru.

9. **Jaká je podle Vás ideální prevence problematiky kybernetické bezpečnosti?**

Bohužel žijeme ve světě, kdy je kyberprostor neoddělitelnou částí našich životů a v podstatě je v dnešní době nepostradatelný. Je to zásadní prvek komunikace, při hledání práce, při vyhledávání a objednávce služeb, při zachování vzpomínek formou zálohovaných fotografií, při platbách a získávání informací. Předávání informací dětem a dospívajícím je z pozice rodiče nutné, ale zároveň nedostačující. Rodiče tomu totiž "nerozumí". Děti a dospívající těmto "nevyžádaným radám" málokdy přikládají důraz. Ve škole by tomu určitě měla být věnován čas. Ať už při hodinách IT nebo v rámci přednášek. Tam by jim mohli uvádět případy, které se opravdu staly a jak nepříjemné, či fatální následky to mělo. Pokud by to v rámci přednášky zaznělo ze strany policie, která takové případy v rámci kriminality řeší, určitě by to mělo váhu. Také by je tedy měli informovat zdroje, které jsou pro ně zajímavé, a to například influenceři, slavné osobnosti.

Vyhodnocení rozhovorů s rodiči

Z rozhovorů vyplynula bezpochyby výborná zkušenost a informovanost vybraných rodičů v oblasti kybernetické bezpečnosti. Sami mají hodně zkušeností s kybernetickými útoky z pozice oběti a dokázali si s řešením velice dobře poradit.

Oba rodiče vnímají kybernetickou kriminalitu jako vážný a narůstající problém, který postihuje různé skupiny včetně dětí a seniorů. První rodič, pracující jako IT analytik, se pravidelně vzdělává a předává své znalosti formou osvěty, přičemž své děti do 10 let kontroluje při používání zařízení. Druhý rodič, asistentka prodeje a provozní vedoucí, má osobní zkušenosti s kyberútoky a spoléhá na své instinkty a znalosti, aktivně informuje své okolí, ale nechává svým dvěma dcerám (15 a 8 let) volný přístup k internetu, přičemž se je snaží pravidelně informovat o bezpečnosti na sítích. Oba rodiče zdůrazňují potřebu včasného a kontinuálního vzdělávání dětí od rodičů, učitelů i populárních osobností.

UČITEL Č.1

1. **Jaká je Vaše pracovní pozice a náplň Vaší práce?**

   učitelka všeobecně vzdělávacích předmětů na SŠ, vyučování ICT

2. **Jak vnímáte kybernetickou kriminalitu?**

Myslím si, že velká část kybernetické kriminality vyžaduje alespoň určitou součinnost oběti. Často se jedná o různé scamy, phishing a podobné typy útoků, kterým lze předejít kritickým přemýšlením, proto je důležité, aby v této oblasti rostla informovanost a lidé byli schopni podvody rozpoznat.

3. **Předpokládám, že jste se už někdy setkal/a s kybernetickým útokem, jak jste se v této situaci zachoval/a?**

Ano, ale ne osobně (jsem opatrná a učím ICT, takže si vím rady, poznám podvod a používám veškerá možná preventivní opatření.) Kolegyně si do počítače stáhla virus a zpanikařila, takže počítač prostě jen zaklapla a dělala, že se nic nestalo, jen se mi zmínila. Situaci jsme následně vyřešili reinstalací OS.

4. **Účastnil/a, nebo se pravidelně účastníte vzdělávání v problematice kybernetické bezpečnosti? (Např. Školení, kurzy, e-learning apod.)**

   Několika jsem se nějakého školení účastnila, ale ne pravidelně.

5. J**akým způsobem získané informace předáváte dál? (Děti, dospívající, kolegové a další osoby ve vašem okolí)**

Studentům v průběhu výuky, kolegům v průběhu dobrovolných školení, který občas pořádám, dalším osobám, když zrovna nastane příležitost.

6. **Jaká je podle Vás ideální prevence problematiky kybernetické bezpečnosti?**

Rozhodně by měli nejvíce informací předávat učitelé, ale nejen ti, co učí ICT. Věřím, že pokud se budou všichni učitelé, ale ideálně i rodiče a další dospělí, chovat zodpovědně a k práci s internetem, počítači a v kyberprostoru přistupovat bezpečně, děti to odpozorují a budou replikovat.

7. **Je kybernetická bezpečnost obsažena v osnovách výuky ve Vaší škole?**

Ano, v každém ročníku se jí věnuje alespoň pár hodin.

UČITEL Č.2

1. **Jaká je Vaše pracovní pozice a náplň Vaší práce?**

Jsem učitelem na pražské základní škole, učím francouzštinu a informatiku na druhém stupni a robotiku na prvním stupni.

2. **Jak vnímáte kybernetickou kriminalitu?**

Jako vysoce podceňovanou. Je pravda, že jako žák jsem při hodinách informatiky byl vystaven nějakým edukačním videím o tom, jak se bezpečně pohybovat na internetu, ale pokud neprobíhá diskuze se žáky, přijdou mi taková videa bezpředmětná.

3. **Předpokládám, že jste se už někdy setkal/a s kybernetickým útokem, jak jste se v této situaci zachoval/a?**

Přibližně před rokem uniklo několik mých hesel a jelikož jsem byl hloupý a říkal si, že přece "učiteli informatiky se nic takového nemůže nikdy stát", tak jsem neměl dostatečně zabezpečený ani e-mail, a útočník se tak dostal jednoduše k mým všem účtům, změnil hesla a mailové adresy. Většinu účtů jsem díky rychlému zásahu získal do 24 hodin zpět, nejsložitější byla situace u Facebooku, který pro ověření totožnosti žádal naskenovat občanský průkaz a celý případ se táhl přibližně týden.

4. **Účastnil/a, nebo se pravidelně účastníte vzdělávání v problematice kybernetické bezpečnosti? (Např. Školení, kurzy, e-learning apod.)**

Neúčastním, popravdě ani v mém okolí takové možnosti nezaznamenávám.

5. **Jakým způsobem získané informace předáváte dál? (Děti, dospívající, kolegové a další osoby ve vašem okolí)**

Blízké členy rodiny se snažím v dané problematice poučit a samozřejmě toto téma zařazuji průřezově i do hodin informatiky na základní škole.

6. **Jaká je podle Vás ideální prevence problematiky kybernetické bezpečnosti?**

Myslím si, z nejlepší způsob je ukazovat reálné případy ideální od lidí, kteří jsou pro děti známé - influenceři, youtubeři atd. Je potřeba v nich vyvolat pocit, že i takovým lidem se může stát velká nepříjemnost, pokud budou brát zabezpečení jejich soukromí na lehkou váhu.

7. **Je kybernetická bezpečnost obsažena v osnovách výuky ve Vaší škole?**

Ano, je obsažena v osnovách pro 6. ročník.

Vyhodnocení rozhovorů s učiteli

Oba učitelé zdůrazňují důležitost informovanosti a prevence v oblasti kybernetické bezpečnosti, i když jejich přístupy se liší. První učitelka učí ICT na střední škole, je dobře obeznámena s hrozbami a věnuje se prevenci ve výuce i při školeních pro kolegy. Považuje kritické myšlení za klíč k prevenci útoků, a to nejen pro ICT učitele, ale i pro ostatní pedagogy a rodiče. Druhý učitel, vyučující na základní škole, vidí kybernetickou kriminalitu jako podceňovanou a zdůrazňuje potřebu reálných příkladů od známých osobností k zvýšení povědomí mezi žáky. Má osobní zkušenost s kybernetickým útokem, ale neúčastní se pravidelně školení. Oba se shodují, že kybernetická bezpečnost je součástí jejich školních osnov.

POLICISTA Č.1

1. **Jaká je Vaše pracovní pozice a náplň Vaší práce?**

Preventista Policie České republiky.

Besedy, přednášky a edukace jednotlivých skupin tématy dle aktuálních rizik ohrožující danou skupinu obyvatelstva.

2. **Jak vnímáte kybernetickou kriminalitu?**

Kybernetická kriminalita v současné chvíli patří mezi nejvíce rozšířené nebezpečí ohrožující všechny věkové kategorie a je nutné se jí zabývat jak ze strany prevence vycházející ze státního aparátu a veřejných společností, tak primárně v domácím prostředí ze vzájemného sdílení informací o jednotlivých druzích kyberkriminality a možnosti ji včas rozpoznat a úspěšně se jí bránit.

3. **Předpokládám, že jste se už někdy setkal/a s kybernetickým útokem, jak jste se v této situaci zachoval/a?**

Ano, setkal a několikrát. Tyto útoky převážně vychází z podobných legend a víceméně volající postupuje dle jednotlivých algoritmů dle odpovědí cílové osoby a jedná se o snahu posluchače či čtenáře buď vystrašit, anebo jej nalákat. Většinou se jedná o snadný přivýdělek peněz či jiné rychlé zbohatnutí, neoprávněná odchozí platba z účtu volaného, odsouhlasení vzdáleného přístupu k osobním datům či bankovních účtu apod. Důležité je zachovat chladnou hlavu a rozum do hrsti.

4. **Účastnil/a, nebo se pravidelně účastníte vzdělávání v problematice kybernetické bezpečnosti? (Např. Školení, kurzy, e-learning apod.)**

Ano, v rámci své profese absolvuji pravidelné besedy a dohledávám si aktuální informace od kolegů kriminalistů, ať již se jedná o známé typy kyberútoků, tak i ty nové, doposud veřejnosti zcela neznámé.

5. **Jakým způsobem získané informace předáváte dál? (Děti, dospívající, kolegové a další osoby ve vašem okolí)**

Realizujeme pravidelné edukační besedy pro dané cílové skupiny.

6. **Jaká je podle Vás ideální prevence problematiky kybernetické bezpečnosti?**

Podle mě je současný systém prevence nastaven ze strany státních složek a institucí na velice vysoké úrovni. Problém bývá u rodičů, kteří leckdy nejsou pak v následné kontrole nastavených pravidel bezpečnosti zcela důslední, neboť jsou děti snadno ovlivnitelné a zmanipulovatelné.

7. **Jakým způsobem prevence probíhá? Nabízíte své přednášky školám sami nebo si musí škola požádat?**

Oba způsoby jsou v současné době aplikovány. Většinou prevence vychází již z dlouhodobé spolupráce mezi školami a policejní prevencí, kdy pro každý ročník je nastaveno dané téma a dítě si postupně všechna témata osvětlí. Občasně se objeví situace, kdy školy zjistí nějaký akutní problém a ozvou se s akutní žádostí o realizaci preventivní besedy na míru. Přednášky Policie ČR realizuje zdarma.

POLICISTA Č.2

1. **Jaká je Vaše pracovní pozice a náplň Vaší práce?**

Jsem zařazený v rámci Služby kriminální policie a vyšetřování.

Mou pracovní náplní je především kybernetická trestná činnost v souvislosti s mravnostními trestnými činy.

2. **Jak vnímáte kybernetickou kriminalitu?**

Kybernetická trestná činnost je fenoménem, je všude kolem nás a defacto to veškerá trestná činnost se přesouvá právě do kyberprostoru. Nárůst počtu těchto trestných činů, ale i útoků je rapidní a sledujeme ho zhruba již poslední deset let. Takže za mou osobu je to nyní ta kriminalita, na kterou se nejen policie musí zaměřit nejvíce, ale i právě vzdělávání, prevence a my všichni.

3. **Předpokládám, že jste se už někdy setkal/a s kybernetickým útokem, jak jste se v této situaci zachoval/a?**

Setkal a mnohokrát. Jelikož tyto případy přímo řeším, tak je to můj tzv. Denní chléb, ale setkal jsem se s kybernetickým útokem taktéž i v soukromí. Byl napadnut můj účet na sociální síti a jednou

byla napadena má platební karta, respektive byl učiněn pokus o odebrání finančních prostředků z ní. To první se nepodařilo útočníkovi jen kvůli tomu, že mám dvoufázové ověření účtu, co se týče druhé zkušenosti, taktéž kvůli multifaktorovému ověřování plateb k ničemu nedošlo, ale již je to jen potencionální ukazatel toho, že kdybych nemyslel na zabezpečení, stanu se obětí jako mnoho z nás.

4. **Účastnil/a, nebo se pravidelně účastníte vzdělávání v problematice kybernetické bezpečnosti? (Např. Školení, kurzy, e-learning apod.)**

Ano, pravidelně se účastním školení, kurzů a všeho možného, jelikož to vnímám jako velmi důležité. Já sám se účastním vzdělávání aktivně, jelikož jsem externí vysokoškolský pedagog a taktéž činím mnoho přednášek v rámci vzdělávání rodičů a dětí právě v této oblasti.

5. **Jakým způsobem získané informace předáváte dál? (Děti, dospívající, kolegové a další osoby ve vašem okolí)**

V rámci své profese se převážně snažíme edukovat hlavně policisty, jelikož i v mé náplni práce je metodika a edukace, co se týče vysokoškolské výuky, snažím se studentům ukazovat příklady z praxe a bavit se s nimi o tom, co je aktuální. Co se týče pak „volnočasových" přednášek, vzdělávám hlavně děti a rodiče, protože to je alfa-omega všeho.

6. **Jaká je podle Vás ideální prevence problematiky kybernetické bezpečnosti?**

Ideální forma prevence? Je to souhrn defacto všeho možného. Dle mého je nejdůležitější, aby prevence začala v momentě, kdy se dítě dostane k mobilu nebo počítači a má přístup k internetu, tady dle mých zkušeností prevence hlavně ze stran rodičů fatálně selhává, když tohle řeknu rodičům v rámci přednášek, mají mě za blázna, ale opak je opravdu realitou. Každým dnem se setkávám s tím, že jsou zneužity naše děti ve velmi brzkém věku, které jsou aktivní na sociálních sítích a vůbec nemají ponětí, co je v tomto světe čeká. Mluvím o věkové hranici opravdu 6-10 let, kde vidím úplně největší riziko. Starší děti jsou taktéž velmi rizikové, avšak již nějaké povědomí o kybernetické trestné činnosti mají a je třeba je prohlubovat. Abych to nějak shrnul a neřekl nějaký elaborát na x stran, dle mého názoru prevence ze strany rodičů selhává a není taková, jaká by měla být, když už je, většinou přichází pozdě, samozřejmě, že se najdou výjimky. Prevence ze strany škol taky není ideální, dle mého názoru by se děti neměly v informatice učit jen nějaký word či excel, ale právě bezpečnost v oblasti kyber, protože třeba mobil používají x hodin denně. Podle mě tady selhává i systém, kdy vím, že třeba v Belgii opravdu děti už na prvním stupni učí internetové bezpečnosti, sexualitě a podobně, přičemž osobně bych byl velmi rád, kdyby něco takového bylo i v ČR, jelikož to považuji jako velmi důležité. Samozřejmě i policie

činí preventivní opatření v oblasti prevence, avšak je nutné si uvědomit, že je to složka i represivní. Dále je mnoho neziskových organizací, které působí v této oblasti, to považuji za velmi dobré. Abych to shrnul úplně, prevence v ČR je dle mého názoru na dobré úrovni, ale vůbec ne na ideální. Musíme všichni nějakým způsobem začít od sebe tak, abychom nedávali kyberútočníkům „laciné“ terče ve formě našich dětí, mobilů, finančních prostředků.

Vyhodnocení rozhovorů s policisty

Oba policisté vnímají kybernetickou kriminalitu jako závažné a rozšířené nebezpečí, které rychle roste a zasahuje všechny věkové kategorie. Preventista Policie ČR se zaměřuje na edukaci a prevenci prostřednictvím besed a přednášek, a zdůrazňuje důležitost sdílení informací v domácnostech a mezi kolegy. Pravidelně se vzdělává a považuje státní preventivní programy za efektivní, i když upozorňuje na nedostatečnou důslednost rodičů. Kriminalista se specializuje na kybernetickou trestnou činnost, především ve spojení s mravnostními delikty, a vnímá přesun trestné činnosti do kyberprostoru jako fenomén posledních deseti let. Pravidelně se setkává s kyberútoky jak v práci, tak v soukromí, a zdůrazňuje důležitost multifaktorového ověřování. Aktivně se účastní školení a vzdělávání, a své znalosti předává nejen kolegům, ale i studentům, rodičům a dětem. Kritizuje selhání prevence ze strany rodičů a škol a navrhuje zavést do výuky více informací o kyberbezpečnosti.

Oba se shodují na tom, že prevence kybernetické kriminality musí začínat od útlého věku a že současný systém prevence v ČR je dobrý, ale ne ideální. Prevence by měla zahrnovat nejen státní a školní programy, ale také důslednou kontrolu a edukaci v domácnostech, aby se předešlo zneužití dětí a dalších zranitelných skupin.

Srovnání všech rozhovorů

Z rozhovorů vyplývá, že všichni zúčastnění – rodiče, učitelé i policisté – vnímají kybernetickou kriminalitu jako vážný a rostoucí problém. Rodiče mají různou úroveň zkušeností a přístupů k prevenci, od přísné kontroly po volný přístup s informováním o rizicích. Rodiče se však přiklání k tomu, aby informace předávaly v největším množství učitelé. Učitelé se zaměřují na vzdělávání kybernetické bezpečnosti okrajově a považují za nejlepší způsob, jak předávat informace, pomocí prezentací reálných případů ideálně od slavných osobností (např. influencerů). Policisté kladou důraz na preventivní

programy a spolupráci se školami. Všichni zdůrazňují potřebu včasného a kontinuálního vzdělávání v kybernetické bezpečnosti jak mezi rodiči, pedagogy a policisty, tak i předávání těchto informací dětem a žákům, nebo studentům školních zařízení.

4.4. Celkové vyhodnocení výzkumného šetření

Výzkumné šetření zaměřené na rodiče, učitele a policisty se soustředilo na povědomí a zkušenosti s kybernetickými útoky, prevencí kybernetické kriminality a vzdělávání v kybernetické bezpečnosti. Šetření zahrnovalo dotazníkové šetření a rozhovory s vybranými respondenty. Cílem výzkumu bylo zjistit, jak jsou respondenti informováni o bezpečnostních rizicích, jaké mají zkušenosti s kybernetickými útoky a jak řeší tyto situace. Výzkum byl zaměřen na prevenci a vzdělávání v oblasti kybernetické bezpečnosti, s cílem zlepšit povědomí a snížit počet obětí kybernetických útoků.

Na základě výsledků dotazníku a rozhovorů je zřejmé, že osvěta a vzdělávání v kybernetické bezpečnosti je velice důležité pro přecházení a snadné řešení rizik v kyberprostoru. Vzdělávání této problematiky by mělo být nejvíce zaměřené ze strany rodiny a učitelů. Z rozhovorů se zástupci rodičů, učitelů a policistů vyplynuly následující klíčové body týkající se vzdělávání a prevence v oblasti kybernetické bezpečnosti, které nám odpovídají na výzkumnou otázku č. 1 **Jak probíhá vzdělávání a prevence v oblasti kybernetické bezpečnosti?**

- Rodiče mají značné osobní zkušenosti s kybernetickými útoky, což posiluje jejich uvědomění a snahu informovat své děti a okolí. Zdůrazňují důležitost včasného vzdělávání o kybernetické bezpečnosti od útlého věku. Pravidelně předávají své znalosti a zkušenosti, a to především v rámci rodiny, i když uznávají, že není vždy možné kontrolovat všechny aspekty digitálního života svých dětí. Zdůrazňují, že kromě rodičů by měli být do vzdělávání zapojeni také učitelé a populární osobnosti, protože děti a dospívající často více reagují na rady od osobností, které respektují. Rodiče používají různé formy osvěty a příkladů ze skutečného života k vysvětlování rizik. Mají však rozdílné přístupy k monitorování aktivit svých dětí na internetu, od přísné kontroly u mladších dětí po otevřenější diskusi a informování u starších.
- Učitelé na středních i základních školách začleňují kybernetickou bezpečnost do svých osnov, přičemž používají praktické příklady a situace, aby zvýšili povědomí mezi studenty. Důraz je kladen na kritické myšlení jako klíčový nástroj k rozpoznání podvodů a kybernetických hrozeb.

Podle Učitele 1 by informace o kybernetické bezpečnosti měli předávat nejen učitelé ICT, ale všichni pedagogové a také rodiče.

- Policie organizuje preventivní besedy a přednášky pro různé cílové skupiny, což je považováno za efektivní způsob, jak zvýšit povědomí o kybernetických hrozbách. Policisté zdůrazňují, že kybernetická kriminalita je jedním z největších současných rizik, a proto je nezbytné, aby byla prevence systematicky zahrnována do vzdělávacích programů. Existuje dlouhodobá spolupráce mezi školami a policejní prevencí, kde jsou preventivní aktivity součástí školního vzdělávání. Policie reaguje i na akutní potřeby škol, které mohou požádat o speciální besedy při zjištění konkrétních problémů. Policisté však vidí problém v nedůslednosti některých rodičů při aplikaci a kontrole bezpečnostních pravidel, což může vést k vyšší zranitelnosti dětí vůči kybernetickým útokům.

Výzkumná otázka **č. 2 Jakou mají respondenti zkušenost s kybernetickými útoky?**

Jak jsme už zjistili z výsledků dotazníkového šetření a rozhovorů, většina respondentů se s kybernetickými útoky setkala. Nejčastější byl SPAM a PHISHING, HOAX a REVERZNÍ INZERTNÍ PODVOD byly v závěsu v počtu odpovědí. S cíleným útokem na konkrétní osobu jako KYBERŠIKANA, KYBERGROOMING nebo KYBERSTALKING zde byly méně časté, ale stále zde byl počet odpovědí kolem 10 % z celkového počtu.

Výzkumná otázka **č. 3 Jak setkání s kybernetickým útokem respondenti řešili?**

Z odpovědí v dotazníkovém šetření a rozhovorů vyplynulo, že více než polovina respondentů dokázala samostatně rozpoznat a zastavit kybernetický útok. To naznačuje, že mají dobré povědomí a schopnosti v oblasti kybernetické bezpečnosti. Přesto značný počet respondentů situaci vůbec neřešil, což může ukazovat na neznalost správných postupů nebo podceňování závažnosti útoků.

Malý počet respondentů nahlásil incident na Policii ČR, což naznačuje potřebu většího povědomí o možnostech právní ochrany a také zvýšení důvěry v policii. Někteří respondenti se obrátili na své blízké, což je také důležitý krok pro zajištění podpory a poradenství. Celkově je zde prostor pro zlepšení v oblasti informovanosti a reakce na kybernetické útoky.

Na základě rozhovorů s rodiči, učiteli a policisty však můžeme identifikovat několik **klíčových mezer ve vzdělávání** a prevenci v oblasti kybernetické bezpečnosti:

1.Nedostatek pravidelného a strukturovaného vzdělávání pro rodiče a veřejnost

Rodič 2 se nezúčastňuje žádných školení a spoléhá na své instinkty a znalosti. Rodič 1 i Policista 1 zdůrazňují důležitost osvěty, ale přiznávají, že osvěta často přichází pozdě. To naznačuje potřebu strukturovaných a pravidelných informačních kampaní.

2. Nízké zapojení škol do systematického vzdělávání o kybernetické bezpečnosti a nedostatečné množství informací o kybernetické bezpečnosti ve výuce

Učitel 2 zmiňuje, že i když se kybernetická bezpečnost probírá v osnovách, výuka je často povrchní a chybí hlubší diskuse a reálné příklady. To naznačuje potřebu zlepšení metod výuky.

Učitel 1 potvrzuje, že kybernetická bezpečnost je v osnovách, ale věnuje se jí jen pár hodin ročně, což není dostatečné pro důkladné vzdělání studentů.

Učitel 1 zdůrazňuje důležitost kritického myšlení, ale také připouští, že ne všichni učitelé mimo ICT věnují tomuto tématu dostatečnou pozornost. Potřeba je tedy začlenit kybernetickou bezpečnost do více předmětů a rozvíjet praktické dovednosti.

Policista 2 poukazuje na fakt, že vzdělávání a prevence jsou klíčové, ale současný systém vzdělávání může být nedostatečný v praxi.

3. Nedostatečné zapojení rodičů do kontroly a vzdělávání dětí

Rodič 2 nechává své děti volně přistupovat k internetu bez sledování jejich aktivit, což může vést k větším rizikům. Policista 1 uvádí, že rodiče často nejsou důslední v kontrole bezpečnostních pravidel. Policista 2 pak ze svých zkušeností konstatuje, že prevence a vzdělávání dětí ze stany rodičů fatálně selhává. Tyto informace naznačují potřebu lepšího zapojení rodičů do vzdělávání dětí o kybernetické bezpečnosti a ochotu ke zvýšení jejich povědomí v problematice kybernetické bezpečnosti.

4. Nedostatečnost vzdělávání učitelů v kybernetické bezpečnosti

Učitel 2 zaznamenal nedostatek dostupných školení pro učitele. To naznačuje potřebu větší dostupnosti, propagace a pravidelnost školení kybernetické bezpečnosti pro pedagogické pracovníky.

4.5. Doporučení pro zlepšení vzdělávání kybernetické bezpečnosti

Pokud budeme vycházet ze zjištění z předchozích kapitol této bakalářské práce je vhodné vytvořit seznam doporučení pro rodiče a učitele ke zlepšení prevence a vzdělávání v kybernetické bezpečnosti.

Rodiče:

- Rodiče by v první řadě měli pracovat na důvěře mezi nimi a svými dětmi. Důvěra a navození bezpečného prostředí je klíčové pro respektování rad z jejich strany a ochotu dětí s nimi komunikovat a svěřovat se s případnými problémy
- Rodiče by měli mít ochotu se stále sami informovat o možnostech ochrany proti kybernetickým útokům, aby tyto informace a zkušenosti mohli sami předávat dětem v té nejlepší formě. Rodiče tyto informace mohou získat například z ověřených zdrojů již zmíněných preventivních projektů, přednášek policie a nebyla by zde od věci spolupráce se školami ve formě společných debat například o aktuálních problémech v konkrétních školách.

Učitelé:

- Aby učitelé mohli předávat sami informace svým žákům a studentům, je potřeba zavést pravidelné vzdělávání v kybernetické bezpečnosti právě pro učitele. Vzhledem k rychlému vývoji kybernetických hrozeb a útoků bych doporučila podstupovat povinná školení alespoň 2x do roka pro všechny pedagogy
- Bylo by na místě začlenit více informací o kybernetické bezpečnosti do osnov více předmětů a přizpůsobit výklad všem věkovým kategoriím žáků a studentů. Tyto informace je potřeba postupně stále aktualizovat. Žáci a studenti by tak byly více informovaní v oblastech:
  - zabezpečení svých účtů a zařízení,
  - o možných rizicích v kyberprostoru a jak se jim ubránit,
  - rozvíjení praktických dovedností pomocí ukázek reálných situací
  - o tom, že se nemusí bát svěřit učitelům při špatné zkušenosti

Příklad začlenění kybernetické bezpečnosti do různých předmětů:

ICT – jak vytvořit silné heslo, vícefaktorová ověřování, sociální sítě a jejich rizika, základní pravidla při používání internetu, bezpečné chování online

Občanská nauka/ Základy společenských věd – identita občana, digitální komunikace, šikana

Matematika – finanční gramotnost

Právo – trestní odpovědnost, jak postupovat jako oběť trestného činu

Závěr

Tato bakalářská práce na téma Kyberbezpečnost – rizika komunikace na síti se věnovala aktuálním a důležitým otázkám souvisejícím s kybernetickou bezpečností v kontextu rostoucí digitalizace. Bakalářská práce zdůrazňuje závažnost rizik spojených s online komunikací a potřebu prevence a vzdělávání, které jsou klíčové pro ochranu uživatelů před kybernetickými hrozbami a útoky.

Teoretická část poskytla komplexní přehled základních pojmů, typů kybernetických útoků a možné prevence před těmito útoky. Významná role v prevenci a vzdělávání této problematiky náleží rodině, školství a Policii České republiky. Dále jsou zde uvedeny různé organizace a projekty zaměřené na prevenci, vzdělávání a pomoc při řešení rizik v kyberprostoru.

Dle praktické části zaměřené na vzdělávání v kybernetické bezpečnosti ze strany rodičů, učitelů a policistů lze konstatovat, že povědomí o bezpečnostních rizicích v digitálním prostředí je klíčové pro ochranu veřejnosti, zejména dětí a mládeže. Výzkumné šetření ukázalo, že osvěta a pravidelné vzdělávání jsou nezbytné pro prevenci kybernetických útoků. Cíle výzkumu tak bylo dosaženo. Rodiče hrají klíčovou roli v edukaci svých dětí o bezpečném chování online prostřednictvím důvěry a otevřené komunikace. Učitelé se zapojují do výuky kybernetické bezpečnosti, avšak je zde potřeba zvýšit kvalitu a pravidelnost vzdělávání učitelů v této problematice a přenesení informací do výuky. Policejní preventivní aktivity jsou uznávány jako efektivní prostředek k zvýšení povědomí o kybernetických hrozbách.

Pro zlepšení vzdělávání je nezbytné zavést pravidelná školení pro rodiče a učitele, začlenit kybernetickou bezpečnost do více předmětů ve školách a podporovat praktické dovednosti ke zvládání reálných situací v kyberprostoru. Spolupráce mezi školami, rodinami, policií a dalšími organizacemi je klíčová pro budování odolné digitální společnosti, která se efektivně dokáže bránit kybernetickým hrozbám.

Seznam zdrojů a literatury

Knižní zdroje:

ČERNÁ, Alena. *Kyberšikana: průvodce novým fenoménem*. Psyché (Grada). Praha: Grada, 2013. ISBN 978-80-247-4577-0.

GAVORA, Peter. *Úvod do pedagogického výzkumu*. Brno: Paido, 2000. ISBN 80-85931-79-6.

KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 9788088168317.

PRŮCHA, Jan a VETEŠKA, Jaroslav. *Andragogický slovník*. Praha: Grada, 2012. ISBN 978-80-247-3960-1.

SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. Pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. ISBN 978-80-7380-501-2.

ŠAFRÁNKOVÁ, Dagmar. *Pedagogika*. 2. Grada Publishing, 2019. ISBN 978-80-271-1190-9.

ŠEVČÍKOVÁ, Anna. *Děti a dospívající online: vybraná rizika používání internetu*. *Psyché (Grada)*. Praha: Grada, 2014. ISBN 978-80-247-5010-1.

VALIŠOVÁ, Alena a KOVAŘÍKOVÁ, Miroslava. *Obecná didaktika a její širší pedagogické souvislosti v úkolech a cvičeních*. *Pedagogika (Grada)*. Praha: Grada, 2021. ISBN 978-80-271-3249-2.

Legislativa:

Zákon č. 273/2008 Sb. Zákon o Policii České republiky.
In: *Https://www.zakonyprolidi.cz/cs/2008-273*. 2008, 91/2008.

Zákon č. 40/2009 Sb. Zákon trestní zákoník. In: *Https://www.zakonyprolidi.cz/cs/2009-40*. 2009, 11/2009.

Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti. In: *Https://www.zakonyprolidi.cz/cs/2014-181*. 2014, 75/2014.

Elektronické zdroje:

AVAST.COM. *Buď safe online.* Online. Avast. 2020. Dostupné z: https://www.avast.com/cz/besafeonline/. [cit. 2024-06-02].

AVAST.COM. *Víš, jak být na internetu v klidu a v bezpečí?* Online. Buď safe online. 2020. Dostupné z: https://www.avast.com/cz/besafeonline/. [cit. 2024-06-02].

BKB.CZ. *Poslání a činnost.* Online. Bílý kruh bezpečí. 2024. Dostupné z: https://www.bkb.cz/o-nas/poslani-a-cinnost/. [cit. 2024-06-02].

CESKENOVINY.CZ. *Policie loni přijala 2334 lidí, po dvou letech počet policistů stoupl.* Online. České noviny. 2024, 1.2.2024. Dostupné z: https://www.ceskenoviny.cz/zpravy/2473843. [cit. 2024-06-01].

CYBERBLOG.CZ. *Pozor na SIM Swap: nový podvod s appkou mobilního operátora.* Online. Vše o kybernetické bezpečnosti. 2023. Dostupné z: https://cyberblog.cz/mobilni-zarizeni/pozor-na-sim-swap-novy-podvod-s-appkou-mobilniho-operatora/. [cit. 2024-06-11].

DITEKRIZE.CZ. *O Dětském krizovém centru.* Online. Dětské krizové centrum. 2024. Dostupné z: https://www.ditekrize.cz/o-detskem-krizovem-centru/. [cit. 2024-06-02].

EDUKLUB.CZ. *Nebezpečí číhá na síti. O kyberbezpečnosti by se neměli učit jen žáci na školách.* Online. Eduklub. 2024. Dostupné z: https://www.eduklub.cz/2024/01/11/nebezpeci-ciha-na-siti-o-kyberbezpecnosti-by-se-nemeli-ucit-jen-zaci-na-skolach/. [cit. 2024-06-02].

E-BEZPEČÍ.CZ. *Co je kyberšikana?* Online. E-Bezpečí. C2008-2023. Dostupné z: https://www.e-bezpeci.cz/index.php/kontakt/71-trivium/1418-co-je-kybersikana. [cit. 2024-06-11].

E-BEZPEČÍ.CZ. *Co je to stalking a cyberstalking.* Online. E-Bezpečí. C2008-2023, s. 1. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kyberstalking/66-23. [cit. 2024-04-01].

E-BEZPEČÍ.CZ. *Informace o projektu.* Online. E-Bezpečí. 2023. Dostupné z: http://www.e-bezpeci.cz/index.php/o-projektu/oprojektu. [cit. 2024-06-02].

FACEBOOK.COM. *Facebook.* Online. Dostupné z: https://www.facebook.com/. [cit. 2024-06-10].

GOVCERT.CZ. *PODVODNÉ E-MAILY NEBO ZPRÁVY NA SOCIÁLNÍCH SÍTÍCH NA MÍRU: SPEAR-PHISHING A JAK SE PŘED NÍM CHRÁNIT.* Online. NÚKIB. 2020. Dostupné z: https://www.govcert.cz/download/doporuceni/Spear-Phishing.pdf. [cit. 2024-05-27].

INSTAGRAM.COM. *Instagram.* Online. Dostupné z: https://www.instagram.com/. [cit. 2024-06-10].

INTERNETEMBEZPECNE.CZ. *Desatero dobrého "kybernetického" rodiče.* Online. Internetem bezpečně. 2018. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rodice/desatero-dobreho-kybernetickeho-rodice/. [cit. 2024-05-31].

INTERNETEMBEZPECNE.CZ. *Kyberstalking.* Online. Internetem Bezpečně. 2018. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyberstalking/. [cit. 2024-06-11].

INTERNETEMBEZPECNE.CZ. *O projektu.* Online. Internetem Bezpečně. 2018. Dostupné z: https://www.internetembezpecne.cz/o-projektu/. [cit. 2024-06-02].

INTERNETEMBEZPECNE.CZ. *Phishing.* Online. Internetem bezpečně. 2018. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/podvodne-praktiky/phishing/. [cit. 2024-06-06].

INTERNETEMBEZPECNE.CZ. *Sociální sítě.* Online. Internetem bezpečně. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/socialni-media/socialni-site/. [cit. 2024-06-11].

JANÍK, Tomáš a PEŠKOVÁ, Karolína. *Školní vzdělávání: podmínky, kurikulum, aktéři, procesy, výsledky.* Online. Brno: Masarykova univerzita, 2013. ISBN 978-80-210-6396-9. Dostupné z: https://munispace.muni.cz/library/catalog/view/7/3454/1008-1/1#preview. [cit. 2024-06-01].

KAPR, Ondřej. *Podvodná jednání v kybernetickém prostoru z pohledu Policie ČR: Cy3er days.* 2022. – interní dokument pro Policii ČR.

KOPECKÝ, Kamil. *Co je to vlastně ten hoax, dezinformace, misinformace nebo třeba fake news? Čím se tyto termíny liší a co mají společného?* In: E-Bezpečí [online]. 2022 [cit. 2024-04-01]. Dostupné z: https://www.e-bezpeci.cz/index.php/clanky-komentare/2864-co-je-to-vlastne-ten-hoax-dezinformace-misinformace-nebo-treba-fake-news-cim-se-tyto-terminy-lisi-a-co-maji-spolecneho.

KOPECKÝ, Kamil. *Deep fake - stručný úvod do problematiky.* E-Bezpečí, roč. 4, č. 1, s. 23-25. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=1417.

KOPECKÝ, Kamil. *FAKE NEWS - ÚVOD DO PROBLEMATIKY.* E-Bezpečí 2017, 2(2): Page 34-39. Univerzita Palackého v Olomouci. ISSN 2571-1679.

KOPECKÝ, Kamil. *Umělá inteligence.* Online. In: YouTube. 2023. Dostupné z: https://youtu.be/OCdHMXxl3fk?si=9Igh9wFTNvJpw_pE. [cit. 2024-05-19].

KOPECKÝ, Kamil; SZOTKOWSKI, René a DOBEŠOVÁ, Pavla. *Riziková komunikace a seznamování českých dětí v kyberprostoru.* Online. Olomouc: Univerzita Palackého v Olomouci, 2021. ISBN 978–80–244–5915–8. Dostupné z: https://e-bezpeci.cz/index.php/ke-stazeni/odborne-studie/146-rizikova-komunikace-a-seznamovani-ceskych-deti-v-kyberprostoru-2021/file. [cit. 2024-04-01].

KYBEZ.CZ. *Jak vzdělávat v oblasti kyberbezpečnosti na základních a středních školách?* Online. KYBEZ. 2021. Dostupné z: https://kybez.cz/jak-vzdelavat-v-oblasti-kyberbezpecnosti-na-zakladnich-a-strednich-skolach/. [cit. 2024-06-01]

Seznam obrázků

Seznam grafů

Seznam příloh

Příloha č.1 Dotazník

1. Jak byste ohodnotil svou schopnost používat ICT technologie?

Hodnoťte známkou jako ve škole.

1 2 3 4 5

2. Potřebujete k práci na počítači internet?

- Ano, vždy

- Spíše ano

- Spíše ne

- Ne

3. Máte obavu, že byste se mohli stát obětí počítačové kriminality?

- Ano

- Ne

4. Využíváte při práci na počítači také veřejnou síť?

- Ano, nevyužívám

- Ne, nevyužívám

5. Používáte internet pro práci s choulostivými daty? (internetové bankovnictví, komunikace s okolím, posílání intimních fotek apod.)

- Ano

- Občas

- Ne

6.Jaká specifika splňují vaše přihlašovací hesla?

- Minimálně 8 znaků

- Velká a malá písmena

- Číslice a jiné znaky

- Slova nemají spojitost s mou osobou

7. Jaké údaje o sobě uvádíte na sociálních sítích?

- Jméno a příjmení

- Bydliště

- Datum narození

- Fotografie sebe

- Fotografie rodiny

- Povolání

8. Je Váš profil na sociálních sítích veřejný?

- Ano

- Ne

9. Myslíte si, že dokážete rozpoznat kybernetickou hrozbu nebo útok?

- Určitě ano

- Spíše ano

- Spíše ne

- Určitě ne

10. Už jste se někdy setkali nebo stali obětí některého z níže uvedených kybernetických útoků?

- Hoax (poplašná zpráva)

- Spam (distribuce nevyžádané pošty vedoucí k útoku)

- Phishing (snaha získat vaše osobní údaje pomocí falešných zpráv, hovorů nebo e-mailů)

- Kyberšikana

- Kyberstalking (pronásledování pomocí zpráv, telefonátů apod.)

- Kybergrooming (oslovování nezletilých s cílem vylákat je na schůzku a zneužití)

- Reverzní inzertní podvod (snaha získat přístup k platební kartě pomocí oslovení prodávajícího v inzerátu)

- SIM Swap (snaha získat přístup k sim kartě předstíráním mobilního operátora)

- Nesetkal jsem se ani s jedním

11. Pokud ano, jak jste situaci řešili?

- Neřešil jsem to

- Nahlásil na Policii ČR

- Řekl jsem to rodičům, rodině nebo známým

- Útok jsem rozpoznal sám a na poslední chvíli ho zastavil (například blokací nebo nahlášením uživatele nebo čísla)

- Jiné

12. Dozvěděli jste se již v minulosti jak hrozby nebo útoky rozpoznat a jak se bránit? A pokud ano, napište prosím, od koho jste se informace dozvěděli.

Zadejte svoji odpověď

13. Kolik Vám je let?

- 16 - 25

- 26 - 35

- 36 - 45

- 46 a více

14. Vaše nejvyšší vzdělání?

- Základní

- Střední odborné s výučním listem

- Střední odborné s maturitou

- Vysokoškolské

Příloha č. 2 – Odpovědi na otázku č. 12

1	anonymous	Ano, hodně na internetu (Youtube kanály jako Jirka vysvětluje věci apod.)
2	anonymous	Ne
3	anonymous	Nepatral jsem.
4	anonymous	Ano, škola
5	anonymous	Internet
6	anonymous	Internet okoli oolem mne
7	anonymous	Články
8	anonymous	Ne
9	anonymous	Na internetu, přes známé
10	anonymous	Internet
11	anonymous	Ano, webináře, média
12	anonymous	Ne
13	anonymous	Prace
14	anonymous	Ano. Internet, vlastní informovanost, vlastní zkusenosti
15	anonymous	Od banky,z medii
16	anonymous	V rámci své práce - konference, školení
17	anonymous	Ne
18	anonymous	Info na internetu
19	anonymous	Ne
20	anonymous	Ano, internet a v práci
21	anonymous	skoleni, vlastni studium
22	anonymous	škola, rodina, školení, upozornění, selský rozum, internet
23	anonymous	Ne
24	anonymous	Ano, od programátora
25	anonymous	Ano, přednášky na ZŠ

26	anonymous	Ne
27	anonymous	Media
28	anonymous	Hezky v této době podává informace o kyberbezpečnosti PČR
29	anonymous	Ne
30	anonymous	Od kamarádů
31	anonymous	Internet
32	anonymous	Přednáška ve škole od PČR
33	anonymous	Od známých
34	anonymous	Televize
35	anonymous	Z důvěryhodných dostupných zdrojů na internetu
36	anonymous	Média
37	anonymous	Ano, například si změnit heslo. Pokud se jedná o vážnější věc tak nahlásit na policii
38	anonymous	Zkušenosti
39	anonymous	Od učitelů, rodičů a spolužáků
40	anonymous	rodina
41	anonymous	díky prevencím na základní škole a od mamky
42	anonymous	škola, reklamy
43	anonymous	Kovy
44	anonymous	Spise ne
45	anonymous	Kolega
46	anonymous	Ne
47	anonymous	
48	anonymous	IT technik, massmédia
49	anonymous	Internet
50	anonymous	Preventivní videa
51	anonymous	Ne

52	anonymous	Ano, z internetových kampaní
53	anonymous	Neříkat nic osobního, žádné údaje, chtít ověření, závěsit a zavolat napr do banky sám
54	anonymous	Televizní zprávy, YouTube
55	anonymous	Rodina
56	anonymous	Ne
57	anonymous	Ano, v práci jsme měli školení CybSafe
58	anonymous	Internet
59	anonymous	Od banky
60	anonymous	Od rodiny
61	anonymous	ne
62	anonymous	ne
63	anonymous	Zasílané zprávy po mně požadovaly zpětné odeslání kódu. Nahlásil jsem to. Od známého.
64	anonymous	Média
65	anonymous	Ano, z internetu, ze zpráv tv
66	anonymous	Ano - internet, preventivní akce policie
67	anonymous	Internet, známi
68	anonymous	Internet
69	anonymous	Ano,od Pčr
70	anonymous	Ne.
71	anonymous	20ti letá praxe v e-komerci. To se člověk dozví mnohé a musí být velice obezřetný hlavně při komunikaci se zahraničím....
72	anonymous	Internet
73	anonymous	Youtube, IT portaly
74	anonymous	Bezne zdroje, NUKIB, Lupa.cz a jine weby, monitoring zamestnavatele (podnik zamerujici se na IT)
75	anonymous	Ne

76	anonymous	Ve škole
77	anonymous	Ve škole - studuji informační bezpečnosti, v práci - pracuji jako kyberpečnostní analytička v SOC
78	anonymous	Od kantorů ve škole většinou a od rodičů
79	anonymous	V TV pomocí informačních reklam, proškolení v práci
80	anonymous	Yt -> Jirka vysvětluje věci například
81	anonymous	Přednáška ve škole, varující videa na internetu
82	anonymous	Ne
83	anonymous	Ne
84	anonymous	Tak nějak sám. Pracuju s internetem pravidelně tak rozpoznám normální chování webu.
85	anonymous	V praci
86	anonymous	Ne.
87	anonymous	Ano, spíše sám, zkušenostmi, a komunikací s ostatními, ale ve skautu jsme na to měli programy, abychom zkušenosti předali dětem
88	anonymous	ne
89	anonymous	Od IT specialistu PČR
90	anonymous	Ano, obecne dostupne informace v mediich a na internetu.
91	anonymous	Absolvování vzdělávacího bloku kyberkriminalita v rámci s studia
92	anonymous	Nn
93	anonymous	Bylo to vždy průhledné
94	anonymous	Internet
95	anonymous	Z internetu
96	anonymous	Školení, kolegové, net
97	anonymous	Od banky.
98	anonymous	Ano, z veřejného prostoru
99	anonymous	Ne
100	anonymous	Ne

101	anonymous	Je to v mém vlastním zájmu se chránit, tudíž si veškeré informace o tom jak se chránit hledám sám.
102	anonymous	Internet, televize

Příloha č. 3 – Otázky pro rozhovory

Otázky pro rodiče:

1. Jaká je Vaše pracovní pozice a náplň Vaší práce?

2. Jak vnímáte kybernetickou kriminalitu?

3. Předpokládám, že jste se už někdy setkal/a s kybernetickým útokem, jak jste se v této situaci zachoval/a?

4. Účastnil/a, nebo se pravidelně účastníte vzdělávání v problematice kybernetické bezpečnosti? (Např. Školení, kurzy, e-learning apod.)

5. Jakým způsobem získané informace předáváte dál? (Děti, dospívající, kolegové a další osoby ve vašem okolí)

6. Jak staré máte děti?

7. Jak často a jak dlouho je necháváte využívat internet? Máte přehled o jejich aktivitě na internetu a sociálních sítích?

8. Jakým způsobem se je snažíte chránit před kybernetickými hrozbami?

9. Jaká je podle Vás ideální prevence problematiky kybernetické bezpečnosti?

Otázky pro učitele:

1. Jaká je Vaše pracovní pozice a náplň Vaší práce?

2. Jak vnímáte kybernetickou kriminalitu?

3. Předpokládám, že jste se už někdy setkal/a s kybernetickým útokem, jak jste se v této situaci zachoval/a?

4. Účastnil/a, nebo se pravidelně účastníte vzdělávání v problematice kybernetické bezpečnosti? (Např. Školení, kurzy, e-learning apod.)

5. Jakým způsobem získané informace předáváte dál? (Děti, dospívající, kolegové a další osoby ve vašem okolí)

6. Jaká je podle Vás ideální prevence problematiky kybernetické bezpečnosti?

7. Je kybernetická bezpečnost obsažena v osnovách výuky ve Vaší škole?

Otázky pro policisty:

1. Jaká je Vaše pracovní pozice a náplň Vaší práce?

2. Jak vnímáte kybernetickou kriminalitu?

3. Předpokládám, že jste se už někdy setkal/a s kybernetickým útokem, jak jste se v této situaci zachoval/a?

4. Účastnil/a, nebo se pravidelně účastníte vzdělávání v problematice kybernetické bezpečnosti? (Např. Školení, kurzy, e-learning apod.)

5. Jakým způsobem získané informace předáváte dál? (Děti, dospívající, kolegové a další osoby ve vašem okolí)

6. Jaká je podle Vás ideální prevence problematiky kybernetické bezpečnosti?

7. Jakým způsobem prevence probíhá? Nabízíte své přednášky školám sami nebo si musí škola požádat?