VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

POČÍTAČOVÁ KRIMINALITA ZAMĚŘENA NA ZNEUŽITÍ IDENTITY A TRESTNÁ ČINNOST S TÍM SPOJENÁ

Autor práce: Adam Struhovský

Studijní program: Bezpečnostně právní činnost

Forma studia: prezenční

Vedoucí práce: Mgr. Bc. Josef Kříha, PhD.

Katedra: Katedra právních oborů a bezpečnostních studií

2022

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 6, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Adam Struhovský
Studijní program: Bezpečnostně právní činnost
Studijní obor: Bezpečnostně právní činnost ve veřejné správě
Forma studia: Prezenční
Místo studia: České Budějovice

Název bakalářské práce: Počítačová kriminalita zaměřena na zneužití identity a trestná činnost s tím

Název bakalářské práce v anglickém jazyce: Cybercrime Focus on Identity Theft and Related Crime

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, titul):
Mgr. Bc. Josef Kříha, PhD., č. mob. 00420 602 183 463, e-mail: kriha@vsers.cz
Datum zadání bakalářské práce (měsíc, rok): Duben 2021

Cíl bakalářské práce:
Hlavní cíl bakalářské práce má ambici formou širšího teoretického vhledu prvotně objasnit základní pojmosloví a východiska zkoumané tematické oblasti, včetně de lege lata reflexe účinných trestněprávních nástrojů, souvisejících s fenoménem nezákonného zneužití identity, sociálních sítí a související páchané trestné činnosti. Vedlejší cíl empirické části práce v rámci určujícího časového období, formou kvantitativního výzkumného (dotazníkového) šetření bude úžeji demonstrovat a fenomenologicky detekovat stav, strukturu a četnost poukazované krádeže osobních údajů v České republice.

Student: Adam Struhovský	30.4.2021 *datum*	Adam Struhovský *podpis*
Vedoucí práce: Mgr. Bc. Josef Kříha, PhD.	14.5.2021 *datum*	 *podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	11.5.2021 *datum*	 *podpis*
Prorektorka pro studium a vnitřní záležitosti: RNDr. Růžena Ferebauerová	1.6.21 *datum*	 *podpis*
Pověřený rektor: doc. Ing. Jiří Dušek, Ph.D.	1.6.2021 *datum*	 *podpis*

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z.ú.
-2-
ČESKÉ BUDĚJOVICE

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucímu bakalářské práce Mgr. Bc. Josef Kříha, PhD. za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

STRUHOVSKÝ, A. *Počítačová kriminalita zaměřena na zneužití identity a trestná činnost s tím spojená: Bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2022. 75 s. Vedoucí bakalářské práce: Mgr. Bc. Josef Kříha PhD.

Věcná část bakalářské práce (dále jen „práce“) má ambici formu teoreticko-empirického vhledu objasnit celospolečensky odborně aktuální tematickou oblast, vymezující vybraný trestněprávní segment páchané počítačové kriminality a její trestněprávní konsekvence. Práce je rozdělena do osmi kapitol, úvodní část teoreticky orientované „práce“ primárně a rámcově vymezuje historickou genezi vývoje počítačové kriminality a jejich kategorizaci. V širší optice dále poukazuje k vybraným hmotněprávním a procestněprávní ustanovením trestního a správního (přestupkového) práva.

V práci jsou dále úžeji demonstrovány možné formy zneužití identity, jak si pachatel vytváří falešnou identitu a jakými způsoby útočí na svoji potenciální oběť. Práce také řeší problematiku sociálních sítí, jestli jsou bezpečné pro jejich uživatele a jaké nesou s sebou rizika. V šesté kapitole je vymezena viktomologie a prevence počítačové kriminality a sedmé kapitole je psáno o bezpečnostním opatření výpočetní techniky a obranou proti počítačové kriminalitě. Praktická část této práce se věnuje informovanosti Počítačové kriminality na zneužití identity prostřednictvím elektronického dotazníkového šetření.

Klíčová slova: bezpečnostní opatření, prevence, problematika sociálních sítí, zneužití identity

ABSTRACT

STRUHOVSKÝ, A. *Cybercrime Focus on Identity Theft and Related Crime. BachelorThesis.* ČeskéBudějovice: The College of European and Regional Studies, 2022. 75 pp. Supervisor: Mgr. Bc. Josef Kříha, PhD.

The factual part of the bachelor's thesis (hereinafter referred to as the "thesis") has the ambition of clarifying the form of a theoretical-empirical perspective to the socially current thematic area, defining a selected criminal law segment of cybercrime and their criminal consequences. The thesis is divided into eight chapters. The introductory part of the theoretically-oriented "work" primarily and broadly defines the historical genesis of the development of cybercrime and their categorization.. In a wider range, it also points to a selected substantive and transnational law provisions of criminal and administrative (misdemeanor) law.

The thesis also more closely demonstrates possible forms of identity abuse, how the perpetrator creates a fake identity and how he attacks on his potential victim. The thesis also addresses the issue of social networks, whether they are safe for their users and what the risks are. The sixth chapter defines the victimology and prevention of cybercrime. The seventh chapter is written about computer security measures and defense against cybercrime. The practical part of this work is devoted to computer crime awareness of identity abuse through an electronic questionnaire survey.

Key words: identity abuse, prevention, safe measures, social networks issues,

Obsah

Úvod

V dnešním moderním světě se čím dál víc zdokonaluje výpočetní technika a počítačová kriminalita se stala novým fenoménem, který postihl i Českou republiku. Svým charakterem je naprosto odlišná od jiných kriminálních aktivit, se kterým se společnost neustále setkává, protože technologie ovlivnili náš život a komunikaci přes internet, e-mailem, sociálními sítěmi apod. Pachatelé využívají výpočetní techniku jako prostředek ke spáchání trestné činnosti a zneužívají osobní data, dokumenty, informace ke svému obohacení nebo zaútočí nebezpečným *„malwarem*“, který obsahuje nejrůznější formy škodlivých kódů například trojský kůň, vir, červ nebo *„phising*“. Trestné činy jako jsou podvod, krádež, vydírání nabírají novou formu páchání přes moderní technologie a komunikací, která nabírá obrovskou rychlost ve virtuálním světě. V minulosti lidé prokazovali svoji identitu, listinnými dokumenty, takže zcizení listinných dokumentů lidé dokázali rychle zaznamenat, ale v dnešním světě plných moderních technologií vystupujeme virtuálně, naše identita je potvrzována hesly či PIN kódy, které umožňují přístup k našim uživatelským účtům, internetovému bankovnictví nebo vstupu k našim databázím a údajů, které si ukládáme, a jsou pro nás velmi důležité. Zneužití naší identity odcizením našich identifikačních údajů zjišťujeme, až když jsme byli nějakým způsobem poškozeni nebo naše identita byla využita k trestné činnosti pachatelem například nákupem zbraní na černém trhu nebo obchodování s drogami.

Zneužití identity, krádež či podvod není novým jevem, který vznikl, ale jenom dostal novou podobu v nových moderních informačních systémech, které se rychle šíří a páchají velké škody. Důležitou obranou proti zneužití osobních údajů je intenzivní prevence a zabezpečení naší výpočetní techniky, uživatelských účtů, používání antivirové ochrany, abychom předešli útokům, o které se pachatelé pokouší.

1 Cíl a metodika bakalářské práce

Hlavním cílem bakalářské práce primární formou vhledu teoretickou formou objasnit základní východiska a pojmosloví zkoumané tematické oblasti reflektující počítačovou kriminalitu za pomoci řešené podrobné rešerše dostupné literatury a odborných pramenů včetně de lege lata reflexe, účinných trestně právních nástrojů, související osobních údajů ve výpočetní technice, na internetu a sociálních sítí. Vysvětlení problematiky sociálních sítí, jaký mají dopad na jejich uživatele popsat, jak se má zabezpečit aplikace, aby se zabránilo vniknutí do uživatelského účtu a jeho zneužití, kde jsou citlivé informace a řešit co nejrychlejší formou našich soukromých údajů. Vysvětlit bezpečnostní opatření výpočetní techniky, aplikací a proč je dobré si kvalitně chránit svoje osobní informace na počítači, internetu. Doporučit bezpečnostní programy a navrhnout opatření.

Empirická část „práce“ spočívá ve vypracování výzkumného dotazníkového šetření, která má demonstrovat formou empirického monitoringu o počítačové kriminalitě od dotázaných respondentů. Dotazníkové šetření získá poznatky od široké veřejnosti, zda měli nebo mají stále zkušenost se zneužíváním identity, osobních údajů nebo krádeže účtů v aplikacích a jaký systém zabezpečení využívají. Informace z dotazníkového šetření jsou graficky zpracovány a vyhodnoceny v praktické části práce.

2 Historická geneze počítačové kriminality

Rozvoj počítačové kriminality vzniká od vývoje první počítačové technologie, které byli pro společenské využití v administrativě a podnicích v sedmdesátých let. Počítače nebyli mohutně rozšířené do osobního uživatelského vlastnictví. Nejčastějším prvním útokům protiprávního jednání, které akcentovala fyzické poškozování systémů manipulace uložených dat. V České republice první počítačový zločin se uskutečnil v sedmdesátých letech v Úřadu důchodového zabezpečení, kde operátor narušoval funkčnost magnetem záznamy na magnetických páskách. Zaměstnanec byl odsouzen za sabotáž a současně jeho kolega za neoznámení trestného činu.[1]

Dalšími útoky začali útočníci měnit poklady připravené ke zpracovávání počítače a měnit údaje přímo v počítači. Abych uvedl příklad, který se stal v zásilkové službě Magnet, kde zaměstnanec odebíral zboží na adresu své matky a do databáze odběratelů vždy uvedl, že zboží bylo zaplaceno. Těmto útokům se říká „dokladové delikty“, jež spočívaly k zasílání faktur k větším odběratelům a manipulování s výplatami ve mzdových účtárnách, kde zaměstnanec zacházel s penězi nebo zbožím. V dnešní době tyto trestné činy jsou kvalifikovány jako podvod aplikace ustanovení § 209 trestního zákoníku, ve znění pozdějších předpisů[2] nebo zpronevěra podle § 206 trestního zákoníku.[3]

Začátkem osmdesátých let počítačové technologie jsou čím dál tím víc oblíbený a dostupný pro širokou veřejnost, počítačové systémy rostou a s nimi i nová skupina zločinců, kteří cílí na software a provádějí trestnou činnost na právně chráněné vynálezy, protože sítě pachatelům umožňovaly vniknout do počítačového systému, kde šířily škodlivý software a spolu s nimi i viry. V roce 1989 britský inženýr Tim Berners – založil nový web „WWW“ (World Wide Web) je souhrnné označení pro všechnu službu provozovanou prostřednictvím sítě Internet. Základním kamenem „WWW“ je tzv. „hypertext“. Hypertext je systém, který má vzájemnou interakci dokumentů a jsou přístupné s pomocí sítě Internet. Tento prohlížeč umí zobrazit jednotlivé (stránky, obrázky, videa, mapy, zprávy atd.) informace zpřístupněné

[1] KOLEKTIV AUTORŮ, *Kriminalistická problematika při odhalování, vyšetřování a prevenci počítačové kriminality.* Vydavatelství a nakladatelství: Policejní akademie České republiky, Praha, 1997, s. 30, ISBN 80-85981-50-5

[2] ČESKO. Zákon č. 40/2009 Sb., Trestní zákoník, § 209 Podvod, [online]. In *Sbírka zákonů, Česká republika.* 2009, částka 2. Dostupné z WWW: https://www.zakonyprolidi.cz/cs/2009-40?text=209

[3] ČESKO. Zákon č. 40/2009 Sb., Trestní zákoník, § 206 Zpronevěra, [online]. In *Sbírka zákonů. Česká republika.* 2009, částka 2. Dostupné z WWW: https://www.zakonyprolidi.cz/cs/2009-40?text=206

po celém světě. Rychlost výměn informací uživatelů na internetu masivně přibýval, což vedlo i ke zveřejňování takových informací, které jsou trestné např. (šíření dětské pornografie).[4]

Počítačové zločiny na internetu přestávají být maličkostí a začínají se dostávat na mezinárodní trestnou činnost. Státy a mezinárodní organizace dávají větší pozornost problematice trestní činnosti ve výpočetní technice, která se zabývá řešením daných problémů intenzivněji.

[4] TOPRANKER.CZ. *Co je to WWW (word wibe web)?* [online]. [cit. 2021-10-8]. Dostupné z WWW: https://topranker.cz/slovnik/www-world-wide-web/

3 Vymezení základního pojmosloví a východisek zkoumané tematické oblasti

Rozšíření výpočetní techniky a její zavádění vytvořily hmotné domněnky pro vznik určité trestné činnosti související s používáním počítačové techniky. Prostředkem kriminality je počítač a jeho vybavení aplikováno ke kriminálním útokům, ale dokonce může být předmětem samotný počítač nebo informační systém, který je zneužit jednáním pachatele k trestné činnosti. Počítačovou kriminalitu můžeme definovat jako trestnou činnost související s počítači. Pachatelé počítačové kriminality jsou různí. Můžou to být uživatelé, kteří nelegálně sdílejí pirátské kopie filmů nebo hudby, ale i vysoce sofistikované organizace, které se zaměřují na praní špinavých peněz, distribuci drog, zneužití osobních údajů, bankovní podvody, krádeže dat, cílem pachatelů majetkový prospěch.[5]

Mnoha definic se shoduje na faktu, že je zcela nezbytné rozlišit dvě základní kategorie počítačové kriminality. První z nich je přímou počítačovou kriminalitou a trestný čin s využitím počítače. Subjektem trestného činu je přímo počítač, kde může jít o neoprávněné použití zařízení výpočetní techniky, odcizení dat uležených na počítačových mediích, nepovolené kopírování počítačového programu. Nejčastěji přímým terčem útoku počítače je server. V druhé situaci nepřímou počítačovou kriminalitou, kde využití informační technologie slouží pouze jako nástroj trestné činnosti, jde o nepovolené kopírování počítačového programu, odcizení dat nebo neoprávněné použití zařízení výpočetní techniky.[6]

3.1 Druhy počítačové kriminality

Rychlým vývojem výpočetní techniky a zavádění do společnosti se objevuje trestná činnost v těchto sférách. Nejčastěji po celém světě se setkáváme s různými případy počítačové kriminality, kterých je celá řada, avšak vybráno bylo pouze několik zajímavých druhů.

3.1.1 Průmyslová špionáž

Cílem průmyslové špionáže je zjistit informace o technologie, postupech, zaměstnancích, odběratelů a výrobního sortimentu, které používá konkurenční firma

[5] VLČEK, Martin, *Počítače a kriminalita*. Praha: Vydavatelství Academia. Nakladatelství Československé akademie věd, 1989, s. 13-16, ISBN 80-200-0139-5

[6] BÍMOVÁ, Alena, *Počítačová kriminalita a naše doba*. Praha: IDG Czechoslovakia, a.s., 1990, s. 10, ISBN 80-900872-2-1

nebo organizace a využít tyto informace ve svůj prospěch. Zájem také mohou mít na důležitých dokumentech firmy nebo zničení údajů v databázi, to konkurenci pomůže k získání času a obchodních výhod oproti své konkurenci. *„V roce 1987 západoněmecká firma Volkswagen ztratila 260 miliónů dolarů tím, že pachatelé vnikli do výpočetního střediska firmy a způsobili změny v programech obhospodařujících důchody a rozpočet společnosti. V témž roce v Anglii odcizil programátor své firmě magnetické pásky s daty finančního rozpočtu na příštích pět let a předal je konkurenci k využití.*“[7]

Průmyslová špionáž může mít podobu:

- podplácení
- podvod
- vydírání
- pořizování audiovizuálních materiálů
- vynášení výsledků jednání a podpisů smluv
- odposlouchávání
- krádež

V databázi počítačů se shromažďuje velké množství tajných průmyslových informací firem a organizací, některé jsou vysoce chráněné a některé zas mají slabé zabezpečení, kde je jednoduché proniknout. Hrozbou můžou být, také jednotliví zaměstnanci, kteří jsou nespokojený nebo propuštěni. Konkurence firmy může infiltrovat svého zaměstnance do firmy, kterou chce poškodit a obohatit se důležitými informacemi.

Proti těmto reálným hrozbám je potřeba bránit a investovat do bezpečnostních režimů, vzdělávání zaměstnanců a jejich kontrole, fyzická ostraha k hlídání objektů, instalace chytrých bezpečnostních systémů (např. biometrické přístupové systémy, technologie skenování obličejů a otisků prstů). V dnešní době existuje mnoho služeb, které se zabývají bezpečnostní dbají na kompletní propojení a zabezpečení firmy, jejich specialisté jsou vyškolené, vycvičené k rychlému zásahu řešení krizové situace.[8]

[7] BÍMOVÁ, Alena, *Počítačová kriminalita a naše doba*. Praha: IDG Czechoslovakia, a.s., 1990, s. 16. ISBN 80-900872-2-1

[8] Top security, *Průmyslová špionáž se týká malých i velkých firem. Jak se bránit?* [online]. [cit. 2021-11-5]. Dostupné z WWW:https://www.topsecurity.cz/blog/clanek/prumyslova-spionaz-se-tyka-malych-i-velkych-firem-jak-se-branit

3.1.2 Výzvědná činnost

Výpočetní technika z oblasti počítačové kriminality je motivována politicky, kde vede k mnoho trestným činům. Počítač je výborným nástrojem k využití nezákonných tiskovin či letáků, a to přímo na území, kde mají být zneužity. Originální verze tiskovin lze nahrát na úložná zařízení (flash disk, kazeta, pevný disk) a překrýt pro jistotu videovým záznamem a bez podezření pronést přes celní orgány, až za hranice státu a potom vyrobit několik počet výtisků pomocí tiskárny a scannerů napojené na počítači.

K počítači můžeme také připojit telefax za pomocí telefonní linky a mohou být propojena do sítí různých států na světě a sloužit tak k dálkovému přenosu informací a dat a rozmnožování tiskovin. „*Spojení přenosnými linkami zprostředkovávají osoby, které přenášejí záznamy počítačových medií, které jsou potom dále zprostředkovávány. Spojení přenosnými linkami se děje nejčastěji prostřednictvím telefonních linek, které jsou pronajímány a využívány v rámci terminálových a počítačových sítí. Pokud nejsou tyto sítě dostatečně kryty, je možno do nich vstoupit a využívat data, programy i periferní (vstupní i výstupní) zařízení příslušných počítačů.*“[9] Data přenášena rádiovým signálem mohou být odposlouchávána jinými zájemci, a to za pomocí přijímače a mikropočítače. Informace přenášené rádiovými vlnami mají nejčastější charakter navigačních hodnot, novinářských informací a komerčních zpráv. Může také jít o vojenské a diplomatické přenosy, které jsou tajné a neměli by se převádět otevřeně a mít jednoduché šifrovací zařízení do něhož by se útočník snadno dostal.

Politicky motivované případy trestné činnosti jsou známy z USA západní i východní Evropy a dalších rozvojových zemí. „*Stali se i případy terminálového proniknutí do počítačového systému Pentagonu i přímé fyzické napadení jeho výpočetního střediska. Došlo rovněž k pokusům zneužít výpočetní techniku instalovanou na jedné z největších leteckých základem USA*.“[10]

3.1.3 Zcizování informačních souborů

V počítači se shromažďují a ukládají data do pevných disků a cloudů, což je online uložiště, zaznamenávají rozsáhlé soubory informací o různých organizacích,

[9] BÍMOVÁ, Alena, *Počítačová kriminalita a naše doba*. Paha: IDG Czechoslovakia, a.s., 1990, s. 20-21. ISBN 80-900872-2-1

[10] BÍMOVÁ, Alena, *Počítačová kriminalita a naše doba*. Praha: IDG Czechoslovakia, a.s., 1990, s. 21. ISBN 80-900872-2-1

firem zaměstnancích, jejich kontech v bankách, majitelích a osobním životě atd. Veškeré tyto informace se můžou stát předmětem zájmu cizích osob, které nemají žádné oprávnění se s nimi seznamovat. Často pachatelé provádějí útok na paměťové karty ke zcizení těchto informací, kde jsou zaznamenávány. „*Frim Imperial Chemical Industries (ICI) je jedním z evropských průmyslových gigantů s ročním obratem 5 miliard dolarů. Široce využívaná výpočetní technika a informace zpracované v několika databázích mají obrovský význam jak pro vlastní firmu, tak pro konkurenci. Toho využil programátor zaměstnaný v jednom z výpočetních středisek této firmy. O víkendu odjel do ústředí (ICI) v Holandsku a během krátké doby tam odcizil nejcennější finanční data a předal konkurenci. Způsobil tak své firmě ztráty ve výši 100 000 dolarů.“*[11] Informace jsou velkým zájmem pro jiné osoby, které je mohou zneužít určitým způsobem. Každý provozovatel rozsáhlých informací měl mít povinnost a zájem chránit informace a data nejlepším způsobem prostřednictvím programů a opatření, vhodných podle právnických norem.[12]

3.1.4 Majetková trestná činnost

Majetková trestná činnost je nejrozšířenějším druhem počítačové kriminality za pomocí výpočetní techniky, kde pachatelé získávají finanční příkazy k převodu zboží, poskytnutí služeb, manipulace s programy, výplatní částky, falešné objednávky drahých zařízení nebo nečestné jednání s programy.

Existuje několik technik, které pachatel může použít k trestné činnosti, kde pracuje s počítačem, ke které má legální přístup nebo se dostává nelegální cestou do spojovací sítě přímo do databáze počítačů. Mezi jednoduché techniky patří například salámová technika, kde se při velké frekvenci přenosů dat pomalu a postupně berou slabé částky na účet pachatele. Pachatel se nejčastěji skrývá tím, že do programu vsune tzv, logickou bombu, tato metoda se zapne při splnění jednou nebo více logických podmínek v programu, která po vykonání zákroku v pachatelův zisk zničí část programů, dat nebo informací tak, že při odhalení klamu je nemožné zjistit.[13] Při rozdělení mezi úrovně metod a použití na vysoké úrovni je technika trojského koně,

[11] BÍMOVÁ, Alena, *Počítačová kriminalita a naše doba*. Praha: IDG Czechoslovakia, a.s., 1990, s. 13. ISBN 80-900872-2-1
[12] BÍMOVÁ, Alena, *Počítačová kriminalita a naše doba*. Praha: IDG Czechoslovakia, a.s., 1990, s. 14. ISBN 80-900872-2-1

[13] BÍMOVÁ, Alena, *Počítačová kriminalita a naše doba*. Praha: IDG Czechoslovakia, a.s., 1990, ISBN 80-900872-2-1

což je o nelegálních instrukcí do počítačového programu, která přetvoří původní záměr a vytrvale plní správně úkoly pro pachatele a sám podvodné manipulace prováděl. Naprogramování trojského koně může být při výrobě předem zabudovaný do součástí počítače, ale tím pádem samotným pachatelem by byl tvůrce technického hardware počítače. Pachatelé počítačové kriminality jsou nejčastěji šikovní programátoři a přicházejí s novými výzvami, jak překonat bezpečnostní systémy a získat informace k obohacení se, vytvářejí nové metody v tomto směru.[14]

Odcizení výpočetní techniky a neoprávněné užívání patří taky k nejčastějším útokům pachatelům, tak i vlastních zaměstnanců, kteří se na počítač připojují. Samotné komponenty jsou cenným zbožím, které se rozprodávají za účelem dosažení zisku. Majetkové trestné činy najdeme v páté hlavě části druhé zákona č. 40/2009 Sb., trestního zákoníku, ve znění pozdějších předpisů, tj. konkrétních ustanovení §§ 205–232 trestního zákoníku.[15][16][17][18]

3.1.5 Vandalismus a terorismus

Výpočetní technika se také stává předmětem útoků vandalských a teroristických projevů, smyslem útoku je výpočetní středisko a pracoviště s počítači, kdy pachatelé se chtějí pomstít politice a celé společnosti jako celku. Několikrát se stalo, že ve výpočetních střediscích byly úmyslně založeny požáry, proti samotnému počítači nebo byla použita trhavina, či úder těžkým tupím předmětem. Útočníci krátkodobě přerušovali dodávku elektrického proudu. Počítač je předmětem organizovaného zločinu a terorismu. Teroristické skupiny jsou politicky motivováni na útok proti informačním sítím, počítačovým programům a datům, za pomocí počítače. Útok je hlavně namířený za účel zastrašit vládu a obyvatele k podporování sociálních nebo politických cílů. Kyberterorismus se nachází hlavně ve virtuálním světě, ale má velký dopad na reálný svět, protože v dnešní době je společnost čím dál tím více závislá

[14] KOLEKTIV AUTORŮ, *Počítačová kriminalita ochrana výpočetní techniky a dat.* RINGO, Praha 6, v gesci Československé společnosti pro kriminalistiku a Akademie J.A Komenského ČR, 1991, s. 26-27. ISBN 80-900634-0-3

[15] VLČEK, Martin, *Počítače a kriminalita*. Praha: Academia. Nakladatelství Československé akademie věd, 1989, s. 18-19. ISBN 80-200-0139-5

[16]POLICIE ČESKÉ REPUBLIKY, *Majetkové trestné činy*. [online]. [cit. 2021-10-10]. Dostupné z WWW: https://www.policie.cz/clanek/pomoc-obetem-tc-majetkove-trestne-ciny.aspx

[17] ČESKO. Zákon č. 40/2009 Sb. Trestní zákoník, §205 Krádež. [online]. In *Sbírka zákonů, Česká republika.* 2009, částka 2. Dostupné z WWW: https://www.zakonyprolidi.cz/cs/2009-40?text=205

[18] ČESKO. Zákon č. 40/2009 Sb. Trestní zákoník, §232 Poškození záznamu v počítačovém systému a na nosiči a zásah do vybavení počítače z nedbalosti. [online]. In *Sbírka zákonů, Česká republika.* 2009, částka 2. Dostupné z WWW: https://www.zakonyprolidi.cz/cs/2009-40?text=232

na informačních technologiích a s ní i vzniká hrozba kyberteroristických útoků. Nejčastější cíle kyberterorismu je získání přístupu vojenských informací nebo zbraní, které jsou ovládány přes počítač. Vytvoření virusu, který zaútočí na počítačový systém v jaderné elektrárně a může účinkovat jako bomba, kde hrozí obrovské riziko nebezpečí pro stát a jeho obyvatele.

4 Zneužití identity a krádež

Už z dávných dob se pachatelé zajímali o identitu jiné osoby, ale to jen z fyzického hlediska, protože dříve se lidé prokazovali listinnými dokumenty (glejtem, vandrovní knížkou, občanským průkazem a jinými dokumenty), ale vzhledem jak se doba neustále vyvíjí v technologiích a počítačoví svět nás čím dál víc pohlcuje a všichni jsme online, používáme moderní výpočetní techniku je to pro útočníky jednoduší si vybrat svoji oběť a použít její identitu ke svým kriminálním činnostem, zájmům a potřeb.

Existuje několik prostředků, jak pachatel získává citlivé informace v počítačovém světě, nejčastěji odcizením elektronických dat, hesel, přístupových údajů, adresy bydliště, bezpečnostních kódů, PIN, kreditní karty, a to za použití vniknutí do cizího počítače tzv. „hacking“ nebo kopírováním dat „skimming.“ Největší nebezpeční představuje ztracení nebo odcizení osobních dokladů a finanční krádež identity, kdy pachatel zneužije osobní údaje oběti pro přístup k bankovnímu účtu, kreditní kartě, kde má možnost nakupovat zbraně, uzavírat různé smlouvy apod. Takhle oběť může rychle přijít o peníze na svém účtu, ale i zodpovídá za činnosti a různé škody a nést i důsledky mnoha trestných činů, které spáchala cizí osoba. Každý den se setkáváme s útoky na platební karty nebo kódy PIN, protože většina z nás platí, přes kreditní kartu, a lidé dnes nenosí u sebe velké částky hotovosti. Podvodníci instalují na bankomaty čtecí zařízení s miniaturním kamerovým systémem nebo magnetického proužku karet, který pozoruje kód PIN. Když vám někdo ukradne papírové doklady, dá se na to přijít v krátké době, ale pokud šikovný útočník nepozorovaně zkopíruje nebo odpozoruje, nemusíme na to přijít včas a bude už pozdě a škody budou obrovské.[19][20]

Rodné číslo je důvěryhodný symbol osoby, která používá množství institucí, pojišťovny, nemocnice, banky, finanční úřad. Pachatel může zjistit díky tomuto symbolu a osobě citlivé informace o jeho zdraví, práci. V praxi se můžeme setkat s neoprávněným pořizováním kopií osobních dokladů jako například (řidičský průkaz,

[19]POLICIE ČESKÉ REPUBLIKY, *Ztráta Identity.* [online]. [cit. 2021-10-12]. Dostupné z WWW: https://www.policie.cz/clanek/ztrata-identity.aspx

[20]Bezpečný Internet, *Krádež Identity.* [online]. [cit 2021-10-12]. Dostupné z WWW: http://www.bezpecnyinternet.cz/pokrocily/ochrana-prav/kradez-identity.aspx

cestovní pas, občanský průkaz), což jen zvyšuje pravděpodobnost odcizení identity a její páchání trestné činnosti. [21]

Bránit se můžeme podáním trestného oznámení na tyto usnesení podle trestního zákoníku:

§ 182 Porušení tajemství dopravovaných zpráv

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

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

§ 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti[22]

4.1 Sociální inženýrství

„Je způsob manipulace lidí za účelem provedení určité akce nebo získávání určité informace. Ve většině případů útočník nepřichází do osobního kontaktu s obětí. Útoky obsahují prvky přesvědčování a manipulace a jsou vedeny buď náhodně, nebo cíleně na konkrétní osoby.“[23] Pachatelé sociálního inženýrství svoje útoky neustále vylepšují a aklimatizují k prostřední, k dosažení svého cíle používají několik způsobů útoků. Vybírají si buď konkrétní osoby, nebo cílené skupinky obětí, kterou si pozorně vytipují podle pohlaví, věku, zájmů, práci atd.

Hlavním cílem útoku je o získání osobních údajů, hesla, kreditní karty apod. Pachatel osloví svoji oběť přes nástroje, které umožňují zasílání velkého počtu zpráv, která se tváří, jako normální zpráva od přátel.

[21] Internetem bezpečně, *Krádež identity*. [online]. [cit. 2021-10-12]. Dostupné z WWW: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/kradez-identity/

[22] ČESKO. Zákon č. 40/2009 Sb., Trestní zákoník, § 182 - 232. [online]. In *Sbírka zákonů, Česká republika*, 2009 částka 2. Dostupné z WWW: http://zakony.centrum.cz/trestni-zakonik/cast-2-hlava-2-dil-2

[23] KOŽÍŠEK, Martin, PÍSECKÝ Václav. *Bezpečně na internetu průvodce chováním ve světě online*. Grada Publishing, a.s., U Průhonu 22, Praha 7, 2016, s. 37, ISBN 978-80-247-5595-3

Situační příklad č. 1

Ahoj zahlédla jsem tvůj profil na internetu a ráda bych se s tebou seznámila, vypadáš sympaticky a máš hezkou profilovou fotku, domluvíme se na něčem? Můj profil najdeš tady.

Dobrý den, Váš přítel vás doporučil do našeho projektu XY, jako odměnu vám zasíláme kupón v hodnotě XY, který můžete uplatnit v našem obchodě

Čau na tom videu jsi ty?! -> odkaz

Získání hesla od uživatele na Seznam email:

Email je třeba odeslat na adresu get.password@seznam,cz. Jako předmět se musí uvést IA_TrN3. Zpráva musí být přesně v tomto formátu:src: adresa@seznam.cz (vaše adresa, na ni bude zasláno heslo a heslo pro ověření vaší totožnosti) Pozor, je nutné mít schránku Seznam, aby server mohl ověřit přihlašovací údaje!

Tedy pokud chcete zjistit heslo ke schránce josefsiroky@seznam.cz a sami máte email jedlicka@seznam.cz s heslem 484875, pak odešlete zprávu ve znění src: josefsiroky@seznam.cz autb: jedlicka@seznam.cz. Nezapomeňte na předmět ve správném tvaru. Obratem přijde zpět email s heslem ke schránce.

„základem úspěšného „rybaření" je důmyslný a dobře napsaný reklamní text působící na psychiku uživatele – v tomto případě na její „temnější" část. Atraktivní téma útoku na cizí emailovou schránku, kdy následovně můžete překvapit svého známého znalostí obsahu jeho mailů nebo přístupových práv."[24] Pachatel má možnost ovládat funkci webové stránky a taky možnost vypnout komentáře, aby tam nebyli negativní ohlasy.

Útočníkovi jde hlavně o to, aby osoba klikla na přiložené odkazy, které jsou posílány na email, Messenger, do zpráv Facebooku a dalších aplikacích. Tyto zprávy je nejlépe hned zablokovat, dát do spamu a vůbec je neotevírat ani neodpovídat, protože možnému pachateli můžete email verifikovat a otestovat, že je odkaz funkční, který se stane oběťmi dalších nevyžádaných zpráv. Tohle je jedna z mnoha metod sociálního inženýrství, vyjmenuju dalších pár metod, které útočníci používají,

[24] JIROVSKÝ, Václav. *Kybernetická kriminalit: nejen o hackingu, crackingu, virech, a trojských koních bez tajemství*. Grad, Praha, 2007, s. 204. ISBN 9788024715612-8024715619

samozřejmě existuje stovky způsobů, jak získávat citlivé údaje a zneužít je k trestné činnosti.[25]

4.1.1 Vishing

Způsob lákání oběti na podvodný web, skrz telefonní hovory, pachatel snaží přesvědčit oběť, že je osobou, za kterou se vydává jako třeba za zaměstnance pojišťovny, kde je zaregistrována oběť nebo její banka.

4.1.2 Honey trap

Hlavní myšlenkou pachatele je založit si velmi atraktivní profil na sociálních sítích a získávat citlivé údaje přes konverzaci s jinými lidmi, vydává se za jinou osobu.

4.1.3 Baiting

Spočívá v rozmístění několika infikovaných USB flash disků uložená v kancelářích na stolech, jakmile zaměstnance tento infikovaný flash disk použije do svého počítače, může se ihned přetáhnout malware a tím dojde k instalaci viru, který napadne počítač. Pachatel tak dostane přístup a veškeré údaje o informační síti ve firmě. Baiting se dá považovat, jako za trojského koně v reálném světě.

4.1.4 Clickjacking

Funguje jako past na uživatele, základem je lákání uživatelů na webové stránky, kde si můžou spustit film zadarmo nebo seriál, po kliknutí na tyto stránky a pokusu o spuštění filmu na tlačítko přehrát na něj vyskočí několik nových oken s reklamami a přesměrují uživatele na další podvodné stránky

4.1.5 Watering hole

Je podobná metoda jako baiting, která se snaží dostat se škodlivým softwarem do počítače oběti a napáchat velké škody, rozdíl je v tom že sází na cloudová úložiště, her, sociálních sítí.[26]

[25] KOŽÍŠEK, Martin, PÍSECKÝ Václav. *Bezpečně na internetu průvodce chováním ve světě online*. Grada Publishing, a.s., U Průhonu 22, Praha 7, 2016, ISBN 978-80-247-5595-3

[26] BDO Česká republika, *Metody sociálního inženýrství*. [online]. [cit. 2021-11-3]. Dostupné z WWW: https://www.bdo.cz/cs-cz/blog/it-security/brezen-2021/metody-socialniho-inzenyrstvi

4.2 Vytvoření falešné identity

Pachatelé před oslovením si vytvářejí důvěrný atraktivní falešný profil na sociálních sítí, aby jejich oslovení vzbudil v oběť zájem. Používají fotografie jiných lidí, které si najdou na internetu, samozřejmě nesmí to být slavná osoba, kterou všichni znají jako například profilová fotografie populárního zpěváka Justina Biebera nebo slavného bývalého fotbalisty Davida Beckhama. Útočník si vybere k vytvoření falešného profilu sociální sít například Facebook. Použijí fotografie normální osoby, kterou si najdou na images.google.com přetáhnout svou vybranou fotografii do vyhledávače, když taková fotografie, už na webu existuje služba Google Obrázky jí vypátrají, tato služba se používá pro ověření, jestli je snadno odhalitelná nebo si vytipují profil na sociální síti Instagramu cizího člověka, který má normální profil a jenom okopírují jeho fotky. Několik uživatelů nepoužívá na profilu svoji fotografii obličeje, ale můžou tam mít fotku psa, auta, znak automobilu, protože není žádné pravidlo, mít svoji fotografii přímo obličej.

Přidají jiné jméno, Zvolí si nejčastěji používaná a častá jména jako například Petr Novák, Matěj Novotný, protože tato příjmení je u nás v České republice nejčastější a doplní si do popisku zájmy, nastaví věk, která jejich potenciální oběť má stejné. Přidá si fiktivní přátele, aby zvýšil úspěch atraktivity a dojem skutečného člověka. Když už útočník profil má vytvořený a má vytipovanou svoji oběť například nezletilé dítě ve věku 12 až 16 let. V okruhu jeho místa bydliště, kde si najde na sociálních sítí jako je třeba Facebook. Následně svoji vytipovanou oběť osloví otevírací zprávou a zahájí takzvané „lovení“.

Situační příklad č. 2

Ahoj, nejsi náhodou z Českých Budějovic, mám pocit, že jsem tě zahlédl včera u náplavky.

Ty taky hraješ basket?

Mám ráda fotbalisty s roztomilým obličejem, kdy máte další zápas? Ráda bych se zašla podívat.

Čauky, všiml jsem si na tvém profilu, že máš ráda filmy o upírech, chodíš často do kina tady ve městě?

Ta fotografie na úvodce s autem je parádní, ráda bych se s tebou večer projela.

Oslovení bývají taky dost často vulgární, a i se sexuálním podtextem, a když se na toto oslovení jejich oběť nechytí, tak jí můžou napsat z jiného falešného profilu.[27]

Pachatelé musí taky dost rozpoznat, jak komunikují mezi sebou mladí lidé, jaký mají styl psaní. Útočník, co se vydává za dívku ve věku 14 let, nemůže psát stylem učitele českého jazyka a používat, dlouhá souvětí a psát spisovnou češtinou. Bylo by to hodně podezřelé a strašně průstřelné na první pohled, zpráva musí být stručná, jasná nejlépe se smajlíky nebo dalšími emotikony.

4.3 Kybergrooming

Definice kybergroomingu *„Je to takové chování uživatelů internetu, jehož cílem je pomocí internetových komunikačních prostředků a jiných technologií vyvolat v dospělém/dítěti pocit důvěry a prostřednictvím falešné identity ho zneužít nebo vylákat na schůzku. Za kybergrooming může být považováno také zneužití dětí mladistvých k jinému účelu, např. ve jménu terorismu (dítě se stává ve jimi víry teroristou)“*[28]. Pachatel musí nejdřív tedy vzbudit důvěru své oběti, tím že má stejné zájmy, problémy. Vytvoří si falešnou identitu a osloví svoji vytipovanou oběť, používají manipulační a přesvědčovací schopnosti na daného uživatele na sociální síti kde jsou v kontaktu k zasílání intimních fotek za různé odměny například dobití kreditu za 3 nahé fotky, nabídka vstupenek za koncert, zaplacení nového telefonu. Útočník dělá dojem, že má

[27] KOŽÍŠEK, Martin, PÍSECKÝ Václav. *Bezpečně na internetu průvodce chováním ve světě online*. Grada Publishing, a.s., U Průhonu 22, Praha 7, 2016, s. 70-72. ISBN 978-80-247-5595-3

[28] KOŽÍŠEK, Martin, PÍSECKÝ Václav. *Bezpečně na internetu průvodce chováním ve světě online*. Grada Publishing, a.s., U Průhonu 22, Praha 7, 2016, s. 72. ISBN 978-80-247-5595-3

peníze a dobrou práci a je velmi ušlechtilý. „Podle průzkumu společnosti Seznam.cz, která mapovala chování lidí na sociálních sítích, odpovědělo 67 % uživatelů, že jim někdo nabízel finanční odměnu za různé služby. S těmito nabídkami se nejčastěji setkaly dívky do 25 let věku. Třetina oslovených pak má tuto zkušenost z více služeb.[29] Oběť může mít pocit díky těmto nabídkám, že druhé straně na ní opravdu záleží a budují si silný vztah mezi sebou. Vzniká tak emoční závislost ve virtuálním vztahu, kde se oběť svěřila se svými problémy, často děti jsou naivní a mají silné tendence se zamilovat ve vizuálních situacích. Útočník všechny informace si ukládá, hlavně intimní problémy a fotografie, která jim oběť poskytla, a tak dostává pachatel mocnou zbraň do svých rukou, kterou může kdykoliv zneužít ve svůj prospěch, například při vydírání pod výhružkou odeslání daných fotek do školy nebo rodičům, pokud nebude dělat to, co se po něm žádá.

Pachatelé chtějí, aby jejich konverzace byla v tajnosti, a žádají své oběti, aby nikomu neříkali, že spolu jsou v kontaktu. Fáze kybergroomingu se dostává i do fáze nabídky na setkání, kde útočník pozve svoji oběť k sobě domů, hlavním volbou místa jsou taková, kde nemá oběť možnost k úniku nebo se dovolat k pomoci například uzavřený sklep, projíždí v autě v hlubokém lese v přírodě. Kde svoji oběť může sexuálně zneužít.

Kybergrooming se zpravidla vyskytuje na těchto sociláních sítí (Facebook, Messenger, Lidé.cz, Twitter, Badoo, Tinder). Případy kybergroomingu se setkáme ve všech zemích světa, protože tato nebezpečná činnost je velmi vysoká a rozšířená po celém světě, stačí jenom internet a výpočetní techniku.

4.3.1 Případ z Velké Británie

„Moderátor a DJ jednoho britského rádia kontaktoval dvě čtrnáctileté školačky prostřednictvím instant messengeru (MSN, ICQ) a navázal s nimi kontakt. Prostřednictvím webové kamery s dívakami komunikoval, hrál s nimi svlékací poker, hovořil o sexu, realizoval různé neslušné aktivity. S dívkami se také setkal s úmyslem

[29] KOŽÍŠEK, Martin, PÍSECKÝ Václav. *Bezpečně na internetu průvodce chováním ve světě online*. Grada Publishing, a.s., U Průhonu 22, Praha 7, 2016, s. 75. ISBN 978-80-247-5595-3

navázat sexuální kontakt, ke kterému nakonec nedošlo. Muž byl odsouzen na 1 rok vezení a po propuštění se musel zaregistrovat na deset let jako sexuální delikvent.“[30]

4.3.2 Případ z České republiky kyberbgroomer Pavel Hovorka

„Vrah Pavel Hovorka přes služební internet vyhledával mladistvé chlapce ze sociálně slabšího prostředí, zjišťoval jejich zájmy a sliboval jim peníze nebo splnění jejich přání za to požadoval jejich nahé fotografie. Pomocí fotografií a prozrazením jejich sexuálního zaměření pak chlapce vydíral a nutil k orálnímu či análnímu sexu. Svou první oběť získal tak, že jí v červenci roku 2005 namluvil, že vyhrála soutěž „Dítě VIP“. Odměnou byl pobyt v Praze v jeho vrátnici, kde chlapce původem z dětského domova znásilnil. Hovorka využíval k seznamování internetové servery, nejdříve chatoval, pak telefonoval, následovalo pozvání oběti k němu do práce. Soud uznal Hovorku vinným celkem ze sedmi případů pohlavního zneužívání, třinácti případů vydírání. Navíc také ohrožoval výchovy mládeže a ze svádění k pohlavnímu styku. Hovorka byl odsouzen na 8 let vězení.“[31]

[30] E-bezpečí, *Případy kybergroomingu I.*, [vid. 14.2.2009]. [cit. 2022-1-4]. *Rizikové jevy kybergroomingu*. Dostupné WWW:https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kybergrooming/33-112

[31] E-bezpečí, *Případy kybergroomingu I.,* [online vydání 2009-2-15], [cit. 2022-2-10]. Dostupné z WWW:https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kybergrooming/33-112

5 Problematika sociální sítě

Bez internetu a výpočetní techniky by nevznikly sociální sítě, takže sociální sítě jsou službou internetu ve virtuálním prostoru, kde uživatelé si vytvářejí profily buď soukromé, nebo uzavřené a tráví svůj čas komunikací mezi svými přáteli, sdílejí svůj osobní život pomocí fotek, co momentálně dělají, kam jeli na dovolenou nebo pomocí sociální sítě vydělávají peníze a tvoří obsah, který je baví, řeší témata na diskusních fórech například o politice, sportu.

Odhadem dnes existuje přes dvě stě sociálních sítí, které využívá 3,4 miliardy uživatelů to je téměř polovina celosvětové populace, a čísla neustále rostou. V České republice sociální sítě momentálně používá téměř pět milionů lidí. Když se nad tím zamyslíme, tak ano je to až neuvěřitelné kolik lidí denně nesmyslně tráví čas koukání do mobilu svých obrazovek, a to mluvím o hodinách, které jim utíkají z jejich vlastního života. Lidé mají problém se soustředit na jiné činnosti, které jsou mnohem důležitější, bez toho, aby se koukli na svůj telefon a zkontrolovali veškeré notifikace, zahrnující například i zprávy ze sociálních sítích. Z vlastní zkušenosti mohu konstatovat a potvrdit, že je zcela běžné, jak se s vámi dotyčný baví a během toho odepisuje na zprávy někomu, kdo je několik kilometrů daleko. Lidé si zvykli hodně žít online a bavit se ve virtuálním světě a v reálném světě mají problém komunikovat na úrovni, oslovit osobu, která se jim líbí a navázat s ní kontakt. Zvykli si na to, že online je jednoduší dát někomu tzv. lajk neboli „to se mi líbí“ na fotku uživatele nebo poslat fotku své postavy, či obličeje, aby zaujali pozornost, protože flirtovat v realitě je pro ně už složité.[32][33]

Já sám mám také účty na několik sociálních sítích a každý den je používám. Sám přidávám fotky na Instagram, Facebook, bavím se zde s přáteli a koukám co je nového ve světě a v mém okolí, ale vím, jak se na nich chovat a nejsem tam tak často podle aplikace na telefonu, která vám dokáže změřit čas, jak dlouho tam jsme. Sociální sítě jsou postaveny hlavně na formě závislosti a vytvářejí je i psychologové, abychom na tom trávili hodně času, bavila nás.

Sociální sít odměňuje náš mozek, protože během používání dopamin, což znamená neurotransmiter štěstí a chtíče, proto je tak těžké skončit. Mozku

[32] Nebojte se internetu, *Sociální sítě.* [online]. [cit. 2022-2-11]. Dostupné z WWW: https://www.nebojteseinternetu.cz/page/3396/socialni-site/

[33] ŠEVČÍKOVÁ, Anna, *Děti a dospívající online,* Grada Publishing, a. s., U Průhonu 22, Praha 7, s. 55-56. ISB 978-80-247-5010-1

se přirozeně líbí, když je odměňován lajky, pocitem důležitosti, kde se rychle vytvoří závislost. Sociální sítě můžeme přirovnat lehce k drogám, droga nás dokáže zničit fyzicky, psychicky a z finančního hlediska, protože za ní budeme dost utrácet pro potěšení a cena je většinou vysoká. Za používání sociální sítě vůbec nic neplatíme, účet si můžeme vytvořit zdarma a využívat ho, ale jsme závislí na počet lajků, srdíček, komentářů, sledujících a zapomínají uživatelé na svůj osobní život, jak žijí v realitě, protože mnoho lidí na sociálních sítí se cítí být někdo jiný a mají větší ego než v normálním životě.[34]

Každá sociální síť nás sleduje je to tzv. velký bratr, který o nás ví všechno, co vyhledáváme skrz sociální síť, co si prohlížíme, lajkujeme, když označíme polohu, kde se momentálně nacházíme. Když to vysvětlím na jedné konkrétní gigantické sociální síti jako je Facebook tak si můžeme zde zapnout a povolit přístup k fotoaparátu, kameře to ale neznamená to, že Facebook bude používat jen tehdy, kdy mi budeme chtít, ale už má přístup kdykoliv oni budou chtít, můžou si nás vyfotit přes fotoaparát nebo odposlouchávat přes náš mobil, který používáme, a to i když máme Facebook vypnutý. Také vědí, co jste smazali a jaké webové stránky prohlížíte, co jsme si koupili a za jakou cenu. Tohle nebezpeční sociálních sítí není zatím tak aktuální, protože by to společnosti stálo peníze mít najaté týmy lidí, kteří budou sedět a sledovat každého uživatele co momentálně dělá, s kým komunikuje. Chtěl jsem tím jenom říct, že tady ta možnost je a může nastat. Tomuto sledování můžeme ukončit tím, že ve svém facebookovém profilu půjdeme do sekce nastavení a zakážeme přístup mikrofonu, fotoaparátu, poloze, kameře a dalším přístupům.[35]

Mezinárodní sociální sítě:

Facebook – patří mezi největší sociální síť světa, kterou využívá přes 1,5 miliardy uživatelů. Zakladatelem této webové služby je Mark Zuckerberg. Slouží jako interakce mezi uživateli, sdílení obsahu a komunikaci.

Instagram – aplikace slouží ke zveřejňování fotografií a videosekvencí za pomocí grafických úprav, komunikace lidí a propojení fotografií, videí do dalších sociálních sítí.

---

[34] Nebojte se internetu, *Sociální sítě.* [online]. [cit. 2022-2-11]. Dostupné z WWW: https://www.nebojteseinternetu.cz/page/3396/socialni-site/

[35] Jak se Rychle Naučit, *Nebezpečí sociálních sítích, které si neuvědomujete,* [online]. [cit. 2022-3-11]. Dostupné z https://jakserychlenaucit.cz/nebezpeci-socialnich-siti/

Twitter – Uživatelům umožňuje psát krátké zprávy, tzv. tweety o délce maximálně 140 znaků. Tweet sledují jednotlivý uživatelé a reagují na něj.

Tiktok – Nová oblíbená sociální sít, vzniklá v Číně, hlavní roli zde hrají, krátká videa, kde uživatelé tvoří svůj obsah například zábavná videa, karaoke, parodie, akrobatické dovednosti, velká konkurence Facebooku a Instagramu.

Ask.fm. – Tato sociální sít má původ z Lotyšska, fungují zde anonymní nebo neanonymní otázky pokládané uživateli a ten na ně podle libosti odpovídá

Snapchat – jedná se o způsob prezentace fotografie než na Facebooku, uživatel vyfotí nebo nahraje video mobilním telefonem a přepošle svým přátelům, odpovědi jsou fotografie nebo videa, je možné si fotografie uložit do alba pomocí screenshotu, ale v tom případě uživatel uvidí, kdo si jeho video nebo fotografii uložil, také zde nastavit časový limit po uběhnutí 1-10 sekund fotografie nebo video zmizí.

České sociální sítě:

Lidé.cz – Největší česká seznamovací síť, účelem je se zde seznámit a potkat lidi, od roku 2014 se zaměřila i na diskusní fóra.

Spolužáci.cz – setkávání současných i bývalých spolužáků v uzavřených skupinách.

Seznamka.cz – nejstarší česká sociální síť, nabízející seznámení pomocí inzerátů

České sociální sítě se dostali do úpadku nástupem Facebooku a Instagramu, nejsou už tolik populární, ale přesto se tu najdou uživatelé, kteří jsou pořád věrní českým sociálním sítím.[36][37]

5.1 Rizika sociálních sítí

Každý, kdo používá sociální sítě a komunikuje, sdílí zážitky, osobní údaje a dalších mnoho informací na internetu většinou zůstane a nejde to vzít už zpět. Potom se často stává, že útočníci toho využijí ve svůj prospěch a použijí tyto informace k trestné činnosti. Uživatel si musí dobře rozmyslet, co všechno chce zveřejnit o svém životě a soukromí, jak si správně zabezpečí svůj účet na sociální síti.

5.1.1 Kyberšikana

„Kyberšikana (Cyberbullying) je jakékoliv chování, jehož záměrem je vyvést z rovnováhy, ublížit zastrašit nebo jinak ohrozit oběť za pomoci moderních technologiích (zejména pak internetu nebo mobilního telefonu).“[38] Kyberšikana má i jiné formy útoků jedincem nebo skupinou, které jsou například verbální útoky nebo neverbální. Mezi útoky patří krádež identity, vyhrožování, vide a nahrávky oběti.

Pro útočníka hlavním faktorem je anonymita, vystupováním pod falešným jménem či profilem, předplacenou SMS kartou nebo e-mailovým účtem zvyšuje pocit anonymity a posílena odvaha agrese k útoku. Místo útoku ve virtuálním prostředí je těžko rozpoznatelné na rozdíl od klasické šikany, kde dojde k útoku při cestě domů, nebo vysmívání ve třídě, které lze předpokládat. Zatímco útok přes internet, může přijít

[36] KOŽÍŠEK, Martin, PÍSECKÝ Václav. *Bezpečně na internetu průvodce chováním ve světě online*. Grada Publishing, a.s., U Průhonu 22, Praha 7, 2016, s. 24-25. ISBN 978-80-247-5595-3
[37] ECKERTOVÁ, Lenka, DOČEKAL, Daniel, *Bezpečnost dětí na internetu.* Computer Press, Brno, 2013, Albatros Media a. s., Na Pankráci 30, Praha 4, s. 35. ISBN 978-80-251-3804-5
[38] KOŽÍŠEK, Martin, PÍSECKÝ Václav. *Bezpečně na internetu průvodce chováním ve světě online*. Grada Publishing, a.s., U Průhonu 22, Praha 7, 2016, s. 62. ISBN 978-80-247-5595-3

kdykoliv nějakou zprávou či videem například o půlnoci, kdy oběť spí. Velikost internetového světa dává kyberšikana nečekané rozměry, nejčastější prostředek pro páchání kyberšikany je sociální sít například Facebook stačí, aby útočník jedním kliknutím zveřejnil ponižující příspěvek proti své oběti hned se to dostane ke stovkám až k miliónům uživatelům, který tento příspěvek uvidí.[39][40] Kyberšikana z právní kvalifikace je velmi obtížné kvalifikovat a v České republice kyberšikana trestní právo nezná.[41]

5.1.2 Sexting

Sexting je spojení slov sex a textové zprávy, fotografického a video obsahu sesexuálním obsahem prostřednictvím využívání moderních informačních technologií. Obsah je zasílaný v rámci milostného vztahu a má dvě úrovně. Výměna sexuálních fotografií nebo videí s vlastním partnerem nebo i dokonce s neznámými osobami. Obojí je velmi rizikové hlavně v druhém případě, protože fotografie intimních částí těla může být jako zneužití k poškození druhé strany jeho zveřejněním nebo výhružkou, když jejich vztah milostný skončí nebo sexuální obsah posíláme neznámým osobám. V sextingu figurují nezletilé a mladistvé osoby, může být z právního hlediska kvalifikován jako trestný čin. Na sociálních sítí je sexting hodně rozšířený přes různé aplikace jako Facebook, Messenger, ale hlavní aplikací zde figuruje sociální síť Snapchat.[42]

Mezi největší rizika sextingu patří citlivý materiál, který potencionální útočník může zneužít v budoucnu a vyhrožovat své oběti, že zveřejní jeho nahé sexy fotky, pokud pro něj něco neudělá. V případě zveřejněním takové zprávy na sociální sít, je prakticky nemožné smazat, protože snadno ztratíme kontrolu nad šířeným materiálem, který může kolovat na sociálních sítí desítky let a dá se zneužít i po nějaké době od doby zveřejnění. Takové zveřejnění nám může způsobit dokonce ztrátu zaměstnání, naši prestiž a může pachatel využít intimní zprávu k výrobě pornografie.

Posílání intimních zpráv je často oblíbené u dětí v rozmezí jedenácti až patnácti let, kteří nejsou vyzrálí natolik, že si neuvědomují, jaké nebezpečí jím hrozí.

[39] ROGERS, Vanessa. *Cyberbullying, Activities to Help Childern and Teens to Stay Safe in a Texitnt, Twittering, Social Networking World.* Jessica Kingsley Publisher, London, 2010, p. 32. ISB 978-80-7367-984-2

[40] Internetem bezpečně, *Kyberšikana,* [online]. [cit. 2022-3-11]. Dostupné z WWW: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/

[41] ŠALMON, Tomáš. *(Ne)bezpečný internet,* Albatros Media a. s., 2021, s. 65-66

[42] Internetem bezpečně, *Sexting,* [online]. [cit. 2022-3-11]. Dostupné z WWW: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/sexting/

Objevily se i případy, kde nahá fotografie byla poslána ihned přes internet v počátku seznámení s osobou, kterou doposud neznali a nikdy neviděli v reálném životě. *„V roce 2014 zrealizoval tým Centra prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci ve spolupráci s firmou Seznam.cz rozsáhlý výzkum zaměřený na rizika spojená s využíváním internetu v populaci dětí. Projekt byl vytvořen na téma sexting, kde zjistili, že 47 % chlapců a 53 % dívek umístilo svou nahou fotografii na internet, kde byly částečně nazí. Přes internet/mobilní telefon poslalo svou intimní fotografii 60 % chlapců a 40 % dívek.*“[43]

I když v České republice je zákonem povolený pohlavní styk od patnácti let, nesmí se s dětmi až do věku osmnácti let pořizovat žádný intimní materiál jako jsou například fotografie, audio, videa apod. Tento obsah může být definován jako dětská pornografie.[44][45] V současné době je trestný čin šíření dětské pornografie upraven § 192 v trestním zákoníku č. 40/2009 Sb. výroba a jiné nakládání s dětskou pornografií *„Kdo přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, bude potrestán odnětím svobody až na dva roky“*[46] Pokud toto spáchá pachatel jako člen organizované skupiny, dále rozšiřuje dětskou pornografii s cílem získat finanční prospěch, může být potrestán odnětím svobody až na 6 let, v případě mezinárodní organizované skupiny až na 8 let. Další právní kvalifikace § 193 v trestním zákoníku. *„Kdo přijme, zjedná, najme, zláká, svede nebo zneužije dítě k výrobě pornografického díla nebo kořistí z účasti dítěte na takovém pornografickém díle, bude potrestán odnětím svobody na jeden rok až pět let.“* [47][48]

[43] KOŽÍŠEK, Martin, PÍSECKÝ Václav. *Bezpečně na internetu průvodce chováním ve světě online*. Grada Publishing, a.s., U Průhonu 22, Praha 7, 2016, s. 85. ISBN 978-80-247-5595-3
[44] KOŽÍŠEK. Martin, PÍSECKÝ Václav. *Bezpečně na internetu průvodce chováním ve světě online*. Grada Publishing, a.s., U Průhonu 22, Praha 7, 2016, s. 96-100 ISBN 978-80-247-5595-3
[45]Internetem bezpečně, *Sexting,* [online]. [cit. 2022-3-11]. Dostupné z WWW: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/sexting/
[46] § 192 odst. 1 zákona č. 40/2009 Sb., trestní zákoník
[47] § 193 odst. 1 zákon č. 40/2009 Sb., trestní zákoník
[48] ŠÁMAL, Pavel, *Trestní zákoník: komentář. 2.* Vydavatelství a nakladatelství: C.H. Beck, Praha . ISBN 978-80-7400-428-5

5.1.3 Kyberstalking

Znamená komplex chování, při kterým pronásledovatel využívá informační a komunikační technologie k zastrašování, vydírání a obtěžování oběti. Sociální sítě a internet je ideálním prostředníkem k páchání trestné činnosti, která představuje velmi snadný, levný anonymní způsob k pronásledování v kyberprostoru. Definice kyberstalkingu definuje Paul Bocij *„Kyberstalking je jako komplex chování, při kterém jedinec, skupina nebo organizace používá informace a komunikační technologii k obtěžování jiného jedince, skupiny nebo organizace.“*[49] Formy kyberstalkingu jsou různé a je jich několik, kterou formou pachatel pronásleduje svoji oběť.

Nejčastější formy:

- zasílání zpráv SMS
- telefonáty a prozvánění během dne
- vkládání příspěvků na profily sociálních sítí oběti
- kontaktování oběti pod falešnou identitou

Hlavními motivy kyberstalkera jsou vyhrožovat a vydírat oběť, demonstrovat svou sílu a poškodit oběť před společnosti nebo opětovné navázání vztahu po odmítnutí. Kyberstalkeři se objevují v chatovacích místnostech na různých sociálních sítí pod falešnou identitou snažící se oslovit potenciální oběť. Statistické údaje sesbírané za rok 2013 a zpracované největší světovou organizací Working to Halt Online Abuse pro bezpečnou práci na internetu ukazují, že oběti kyberstalkingu jsou nejvíc ženy. Pachatelé kyberstalkingu jsou muži 40 % a 30% ženy, u zbytku není pohlaví neznámé. Nejvíc kyberstalkingu se projevilo přes sociální síť Facebook až 30 %.[50]

Právní kvalifikace kyberstalkingu je vymezeno trestním zákoně pod názvem nebezpečné pronásledování. Celé znění zákona, patřící mezi trestné činy narušující soužití lidí, je upraveno v § 354 Nebezpečné pronásledování *„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, c) vytrvale jej*

[49] Wikisofia, *Cyberstaling*, [online]. [cit. 2022-3-11]. Dostupné z WWW: https://wikisofia.cz/wiki/Cyberstalking
[50] Wikisofia, *Cyberstaling*, [online]. [cit. 2022-3-11]. Dostupné z WWW: https://wikisofia.cz/wiki/Cyberstalking

prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje, d) omezuje jev 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, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.“[51] Okolnosti přitěžující dle § 354 OST. 2 písm. a) trestního zákoníků je ta skutečnost, že uvedený čin je spáchán na dítěti nebo těhotné ženě může pachatel být potrestán odnětím svobody na šest měsíců až tři roky.[52]

[51] § 354 odst. 1 zákona č. 40/2009 Sb., trestní zákoník
[52] ŠAMAL, Pavel, *Trestní zákoník: komentář. 2.* C.H. Beck, Praha. ISBN 978-80-7400-428-5

6 Viktimologické aspekty

Viktimologie vychází z latinského slova „victima“ znamenajíc oběť. Viktimologie je nauka o obětech a věnuje se problematice vztahu oběti k pachateli, trestnému činu, na následky trestného činu a jak pomoci oběti.[53] Oběť se rozumí jako konkrétní fyzická osoba, která byla trestným činem poškozena materiálně, usmrcena, ohrožena na životě a zdraví fyzicky či emocionálně, byla omezena na svých právech. Trestní řád říká v této souvislosti o poškozeném, který je vymezen v ustanovení § 43 trestního řádu.[54] Oběť trestního činu je osoba dotčena trestným činem, ale i za nepřímé sekundární oběti jsou považovány a dotčeny osoby blízké či pozůstalé. V trestněprocesním vztahu může být osoba fyzická tak i právnická osoba.[55]

Viktimologie zkoumá oběti jako konkrétní osoby jejich psychologických charakteristik, ale mezi procesy patří také role obětí v průběhu vyšetřování a soudního projednávání trestného činu. Největší důraz viktomologie klade na pomoc obětem a prevenci viktimizace, jak chránit potencionální oběti před kriminalitou. Viktomologie používá také pojmy jako viktimizace a viktimnost.[56]

6.1 Viktimizace

Viktimizace je proces, kde se stává potenciální oběť ve skutečnou, tento proces je ovlivněn hodně chování oběti, protože se často myslí, že jim se to stát nemůže, tak často provokují a nedávají si pozor, když tráví čas sami v noci na odlehlém místě nebo nepoužívají ochranné prostředky například pepřový sprej. Viktimizace se dále rozlišuje na primární viktimizaci, což je újma způsobená pachatelem a vznikající jako přímý, bezprostřední důsledek trestného činu a sekundární viktimizace znamená druhotná újma, jejímž zdrojem může být pachatel, který vyhrožuje nebo zastrašuje oběť, sociální prostředí kde jsou často výčitky rodičů, pověst oběti utrpí zveřejněním případu bulvárním tiskem atd. Pak tu máme terciární viktimizaci, kdy jedinec není schopen

[53] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, *O významu poznávání obětí trestné činnosti,* [online]. [cit. 2022-4-11]. Dostupné z WWW: https://www.mvcr.cz/clanek/o-vyznamu-poznavani-obeti-trestne-cinnosti.aspx

[54] § 43 odst. 1 zákon č. 141/1961 Sb., trestní řád

[55] VYTOUŠKOVÁ, Petra. *Pomoc obětem (a svědkům) trestných činů-Příručka pro pomáhající profese,* Grada Punlishing a.s., 2007, s. 12-13. ISBN 8024720140, 9788024720142

[56] VELIKOVSKÁ, *Martina. Psychologie obětí trestných činů,* Vydavatelství a nakladatelství: Grada Publishing, a.s. U průhonu 22, 170 00 Praha 7, 2016, s. 22-25. ISBN 978-80-271-9172-7

vyrovnat se s traumatickou záležitostí například neschopnost řídit automobil po autonehodě, nutnost změnit profesi.[57]

6.2 Viktimnost

Tento pojem vyjadřuje počet osob nebo skupiny lidí stát se obětí trestného činu, skupiny osob stávají oběťmi svým věkem, povoláním, profesí, psychickými vlastnostmi nebo sociálními charakteristikami, tak se mohou stát velmi rychlím a žádoucím cílem pro pachatele.[58]

Oběť trestné činnosti spočívající v nelegálním získání a následném zneužití identity se dostávají do složité situace, protože viktimizace se odehrává ve virtuálním světě, kde pachatel prostředníkem výpočetní techniky poškodí oběť přímými finančními škody, kde oběť ztratí všechny své úspory, o závažné důsledky, kdy pachatel může zneužít odcizenou identitu k další páchané trestné činnosti, jako je například obchodování s lidmi, terorismus. Má to takové psychologické důsledky, které hlavně závisí na tom, jak identifikační údaje byly zneužity, které mohou ovlivnit celou rodinu oběti.

Z viktimologického hlediska se nejčastěji stává odcizení a zneužití osobních údajů ve zdravotnictví. Ve zdravotní dokumentaci se objeví lékařské informace o léčbě a operačních zákrocích, které byly vykonány pod falešnou identitou, což ohrožuje pravého pacienta. Hrozí velké riziko, že se stanem obětí trestné činnosti ohrožující a zneužívající naše osobní data a identifikaci.

6.3 Viktimologická prevence

„Prevence bývá charakterizována jako předcházení nežádoucích jevů, tj. jakýsi souhrn aktivit, které mají zajistit včasnou obranu před možnými nepříjemnými následky.“[59] Zaměřuje se na potencionální i skutečné oběti trestných činů, poučuje o tom, jak se mají lidé chovat, aby se nestali potencionální obětí pachatele a svůj majetek nevystavovali zvýšenému nebezpečí či napadení. V každém z nás v našem zájmu je chránit své zdraví či usilovat o dosažení základní vlastní bezpečnosti a bezpečnost svých blízkých. Viktimologická prevence se dělí na primární prevenci,

[57] VITOUŠOVÁ, Petra. *Pomoc obětem (a svědkům) trestných činů-Příručka pro pomáhající profese,* Grada Punlishing a.s., 2007, s. 13-14. ISBN 8024720140, 9788024720142
[58] VITOUŠOVÁ, Petra. *Pomoc obětem (a svědkům) trestných činů-Příručka pro pomáhající profese,* Grada Punlishing a.s., 2007, s. 13-16. ISBN 8024720140, 9788024720142
[59] VELIKOVSKÁ, Martina. *Psychologie obětí trestných činů.* Vydavatelství a nakladatelství: Grada Publishing, a.s., U Průlumu 22, 170 00 Praha, 2016, s. 116. ISBN 978-80-271-9172-7

sekundární prevenci a terciární prevenci, nejdůležitější těchto skupin podle mého názoru je primární prevence, protože jejím úkolem je o vytváření nejlepších podmínek pro celé obyvatelstvo, působí plošně a na každého z nás. Zaměřuje se hlavně na budování zdravé společnosti, jejich institucí, občanů a zdravého životního stylu. Sekundární prevence je hlavně zaměřena na rizikové skupiny a jednotlivce, kde je u nich zvýšená pravděpodobnost ke spáchání trestné činnosti a stáním budoucích pachatelů. Poslední skupinou viktomologické prevence je terciální prevence, která má úkol zaměřit se na předcházení recidivitě, což znamená opakování stejného trestného činnosti a viktimilogické recidivitě u oběti. Také se zaměřuje na skupinky nebo jedince, kteří se v minulosti dopustili trestné činnosti, jako u sekundární prevence i v tom případě jde o přímou strategii prevence kriminality.[60]

„Preventivnímu působení by jistě prospěla zvýšená efektivita v činnosti kontrolních a revizních orgánů a včasnost podnětů k zahájení trestního stíhání. Rychlost procesu vyšetřování, odhalování a potrestání pachatelů počítačové kriminality má značný význam nejen proces poznání objektivní pravdy, ale i pro preventivní působení. Proto je ve všech složitých případech počítačové kriminality nezbytné vytvářet speciální vyšetřovací týmy z řad zkušených, právně i ekonomicky vzdělaných policistů a vyšetřovatelů, orientující se i v oblasti výpočetní techniky.“[61]

[60] TOMÁŠE, Jan. *ÚVOD DO KRIMINOLOGIE,* Grada Publishing, a.s., U Průlomu 22, 170 00 Praha 7, s. 158. ISBN 978-80-247-2982-4

[61] PORADA, Viktor, KONDRÁD, Zdeněk. *Metodika vyšetřování počítačové kriminality.* Policejní akademie České republiky, Praha 1997, s. 42, ISBN 80-85981-75-0

6.4 Preventivní projekty proti počítačové kriminalitě

V České republice vzniká celá řada preventivních projektů proti počítačové kriminalitě, které jsou na vysoké úrovni a patří mezi špičky ledovce v rámci Evropy. Preventivní projekty jsou pro všechny občany a hodně projektů vzniká přímo na samotných školách, protože už hned od začátku děti učí, jak se správně bezpečně chovat na internetu a ve virtuálním světě. Tyto projekty jsou podporovány velkými podniky a některé z nich jsou přiblíženy v následujících podkapitolách.[62]

6.4.1 Seznam se bezpečně!

Tento projekt vnikl kvůli sociální síti Lidé.cz, jak už jsem tu zmiňoval v horních kapitolách, Za úkol projektu je informování uživatele v rizikových seznamování nebo komunikaci s neznámými lidmi a zvyšování informací o dané problematice. Hlavní posun v projektu nastal v roce 2009, kde se natočil film Lidé.cz, Spolužáci.cz, a poslal se všem uživatelům sociálních sítí přes internetový portál Seznam.cz, uběhnul první týden a dokument měl přes milion shlédnutí. Vznikla také poradna stejně s filmem, která hned po přehnání filmu byla plná uživatelů a jejich příběhy. Tento film byl distribuován na všech středních a základních škol, jako doporučující učební pomůcka. Na projekt Seznam se bezpečně! Hodně navazují odborné konference, vzdělání učitelů a žáků. Důležitou cílovou skupinou jsou hlavně děti, které neví, jak moc virtuální svět funguje, ale také se zaměřují široka na rodiče, seniory a učitele.[63]

6.4.2 Preventivní program E-bezpečí

Tento preventivní program je zaměřený na vzdělávání a výzkum s rizikovým chování na internetu, který se specializuje hlavně na kyberšikanu, kyberstalking, hoax, spam atd. a také k informačním technologií, jak je správně využívat a vzdělávat se o nich v běžném životě. Hlavním východiskem projektu je terénní práce s nejrůznějšími cílovými skupinami. Uspořádávají různé přednášky, besedy a mapují nebezpečné jevy a zlepšují prevenci proti útočníkům. Jejich cílovou skupinou projektu E-bezpečí jsou žáci a studenti na základních školách, učitelé a v poslední řadě rodiče. Projekt získal několik oceněná v roce 2009 získal třetí místo v národním kole Evropské ceny prevence kriminality MVČR a různá další, je to certifikovaný projekt primární prevence. Podává pomocnou ruku velkému množství uživatelů na internetu, jak dětem,

[62] KOŽÍŠEK, Martin, PÍSECKÝ Václav. *Bezpečně na internetu průvodce chováním ve světě online*. Grada Publishing, a.s., U Průhonu 22, Praha 7, 2016, s. 114. ISBN 978-80-247-5595-3

[63] KOŽÍŠEK, Martin, PÍSECKÝ Václav. *Bezpečně na internetu průvodce chováním ve světě online*. Grada Publishing, a.s., U Průhonu 22, Praha 7, 2016, s. 114-15. ISBN 978-80-247-5595-3

tak i dospělým a zároveň těm, co se dostali do obtížné situace, tento preventivní program je podporovaný klíčovými ministerstvy, jako je MVČR, MŠMT a Policí ČR.[64]

6.4.3 Bezpečný internet

Projekt vznikl na základě ukázat, jak si zabezpečit internet a jak se perfektně bránit proti útočníkům, virům a další počítačové kriminalitě. Bezpečný internet popisuje a vysvětluje konkrétní rizika jako e-mailová komunikace, platby přes internet, protože denně se na český internet připojují miliony lidí a čím víc budou informováni o nebezpečných rizicích, který projekt bezpečný internet upozorňuje, budou rychle umět reagovat na falešné e-maily, spamy, podvodné nabídky a jiné. Hlavní úkol tohoto projektu je posílit sebevědomý uživatelům a vzdělat české uživatele internetu.[65]

[64] KOŽÍŠEK, Martin, PÍSECKÝ Václav. *Bezpečně na internetu průvodce chováním ve světě online*. Grada Publishing, a.s., U Průhonu 22, Praha 7, 2016, s. 147. ISBN 978-80-247-5595-3

[65] KOŽÍŠEK, Martin, PÍSECKÝ Václav. *Bezpečně na internetu průvodce chováním ve světě online*. Grada Publishing, a.s., U Průhonu 22, Praha 7, 2016, s. 148. ISBN 978-80-247-5595-3

7 Bezpečnostní opatření

Bezpečnost počítače a celkové výpočetní techniky je velmi důležitá, protože každý má ve svém zájmu chránit své informace a svoji výpočetní techniku před několika druhy počítačové kriminality, které jsem popisoval ve třetí a čtvrté kapitole. Bezpeční opatření by měli být co nejkvalitnější, protože bezpečností programy a silná hesla chrání naše informace, bankovní účty, uživatelské profily na sociálních sítí, samotnou výpočetní techniku a počítačovou síť.

7.1 Zabezpečení počítačové sítě

Každý z nás používá internet, který je výborným nástrojem pro komunikaci, vzdělávání, zábavu a obrovským množstvím informací, které nám poskytuje. Prostředníkem internetu je počítač a mobilní zařízení, které jsou v domácí síti připojeny k routeru. Router je důležité síťové zařízení, které plní několik funkcí, jako například poskytuje internetovou síť a také propojuje dvě sítě WAN (wide area network) je rozlehlá síť, jejím úkolem je pokrývat geografické území a ta druhá sít je LAN (místní síť neboli ta naše domácí síť) mezi těmito dvěma síti router provádí informace, říká se tomu datový tok. Nezabezpečený router může pachatel proniknout do naší lokální sítě a napadnout počítače, mobilní zařízení další výpočetní techniku, kde může získat přístup k IP adrese a všechny data, informace dokonce i ke kamerovým zařízením. Získá tak informace, které pak může zneužít k vlastnímu prospěchu nebo k další trestné činnosti.[66]

Výrobce každému routeru je přidělena IP adresa, která je složena se čtyř čísel a oddělených tečkou, má nastavenou výchozí heslo, které je dobré hned změnit po prvním přihlášením silným heslem. Router je vhodné pravidelně aktualizovat a filtrovat připojení nežádoucích zařízení do naší sítě, cizím notebookem nebo mobilem. Některé routery lze nastavit tzv. rodičovskou kontrolu ta určuje čas, kdy se zařízení mohou připojovat k internetu. Dalším zabezpečovacích krokem routeru je mít kvalitní aktivní firewall, který má za úkol bránit místní síť, před hrozbami a kontroluje veškerá data.[67]

[66] E-bezpečí, *Jak zabezpečit počítačovou síť,* [online]. [cit. 2022-3-13]. Dostupné z WWW: https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1651-jak-zabezpecit-domaci-pocitacovou-sit

[67] E-bezpečí, *Jak zabezpečit počítačovou síť,* [online]. [cit. 2022-3-13]. Dostupné z WWW: https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1651-jak-zabezpecit-domaci-pocitacovou-sit

7.2 Zabezpečení počítače

Základem zabezpečení počítače je mít aktualizovaný operační systém Windows, momentálně se používá Windows 11 a také Windows 10. Jejich výrobce Microsoft posílá pravidelná bezpečnostní aktualizace a opravuje nedostatky, instalace aktualizace nezabírá téměř žádný čas jenom klikneme na potvrzení aktualizace a proběhne aktualizace. Potom je dobré používat legální software pro zvýšení bezpečnosti počítače, hodně lidí používá nelegální software a myslí si, jak ušetřili několik stovek korun, tento software je zcela zdarma, ale většinou je k tomuto balíčku přibalený škodlivý vir, který využívá neaktualizovaný operační systém a zvyšuje bezpečnostní riziko. Máme několik výrobců, kteří nabízí kvalitní legální software, který nám brání a zabezpečuje počítač, jen si musíme připlatit, ale za bezpečnost našeho počítače je to dobrá investice podle mého názoru. Výhodné je také mít nainstalovaný antivirový program, který zvýší zabezpečení před viry, škodlivým softwarem a dalších druhů.[68]

Úkolem antivirového programu je hlavně minimalizovat hrozby, které se mohou vyskytnout na kterékoliv webové stránce. Můžeme použít několik antivirových programů jako například Avast Antivirus, Norton AntiVirus, PC Protect, Total AV, za určitou částku, která se pohybuje od pětistovky do jedné tisícovky korun českých na dobu jednoho roku nebo podle každého výrobce, který svůj produkt nabízí.[69]

7.3 Zabezpečení uživatelských účtů

Uživatelské účty je nutné mít zabezpečené kvalitním heslem, které by mělo obsahovat minimálně dvanáct znaků s kombinací velkých, malých písmen s číslicemi a speciálními znaky, které nesouvisí s čímkoliv, kdo by o vás mohl například útočník vědět, jako jsou hesla datum narození, oblíbené auto nebo jména příbuzných či domácích mazlíčků, protože jestli dáváte na své sociální sítě fotky svých věcí, co máte rádi, tak útočníka může napadnout použít k heslu. Zvolte vymyšlené věty a nahraďte diakritiku číslicemi a znaky například „levjekrálzvířat“ přetvoříte v heslo levjek8lzv95at plus přidáme velké písmeno a speciální znak, tím pádem máme vyhráno, heslo je silné a bezpečné. Dobré je také hesla pravidelně měnit podle intervalů jednou za rok, pokud máme heslo dlouhé silné. Pokud se vám ale nechce neustále vymýšlet nová hesla, můžete si pomoct z dostupných programů, které se obecné nazývají generátory hesel a navrhují bezpečná silná hesla, jako program Password Generator je

[68] E-bezpečí, *Jak zabezpečit počítač,* [online]. [cit. 2022-3-13]. Dostupné z WWW: https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1653-jak-zabezpecit-pocitac

[69] KRÁL, Mojmír. *Bezpečný internet: Chraňte sebe i svůj počítač,* Grada Publishing, a.s., Praha 7, 2015, s. 21. ISBN 978-80-247-5453-6

velmi jednoduchý na ovládání a spolehlivý, program stáhnete a na instalujete potom kliknete na tlačítko generovat a přehled hesel vám vygeneruje.[70]

Uživatelské účty k zabezpečení lze používat dvou faktorové ověření, které se používá hlavně v bankovním sektoru a je spolehlivé, znamená to, že pro přístup k online účtu využijeme mobilní telefon po zadání hesla a přihlášení musíme potvrdit speciálním kódem, které nám zašlou SMS zprávou do našeho mobilního telefonu, toto zabezpečení nám zvyšuje bezpečnost a doporučují to každé sociální sítě, jako například Facebook, Snapchat, Instagram, Tinder, Tiktok nebo herní platformy, kde si zakládáme účet. Steam, Battle.net, Origin, Ubisoft. Velký problém představuje, když uživatel používá jedno heslo na všechny svoje služby, útočník by pak mohl se dostat na všechno jeho uživatelské účty a mohl by udělat obrovské škody. Největší chybu, co lidé dělají, že si heslo napíši na kus papírku a vloží si do peněženky ke kreditní kartě nebo k počítači pod klávesnici ano je to složité si zapamatovat několik hesel, ale proto existují na to programy, které slouží k uložení hesel spolu se jmény a účty, takový program je například Password Safe kde v programu vytváříte položky, kde si ukládáte jednotlivá hesla. Programů je několik a jsou k dispozici zdarma stačí si jen vyhledat na internetu a podívat se na doporučení a recenze od lidí, kteří tento program měli možnost odzkoušet.[71][72][73]

7.4 Zabezpečení webové kamery

Webové kamery máme připojené k internetu a jsou součástí lokální sítích v domácnostech. Pro pachatele kamery znamenají jeden z mnoha vstupních bodů do počítačových sítí. Existuje několik důvodů, proč útočník chce ovládnout naši webovou kameru a získat co nejvíc citlivých informací, které použije k trestné činnosti vydírání nebo ke zneužití naší identity a poškozování jiných osob. Často významní lidé si webkamerou kamery přelepují na mobilu nebo notebooku lepící páskou, aby snížili viditelnost na bod mrazu například ředitel americké FBI majitel Facebooku Mark Zuckerberg. Hackeři napadnou operační systém našeho počítače, aby se dostali k naší kameře, probíhá to zpravidla prostřednictvím e-mailu, který obsahuje infikovanou

[70] KRÁL, Mojmír. *Bezpečný internet: Chraňte sebe i svůj počítač,* Vydavatelství a nakladatelství: Grada Publishing, a.s., Praha 7, 2015, s. 25-28 ISBN 978-80-247-5453-6
[71] KRÁL, Mojmír. *Bezpečný internet: Chraňte sebe i svůj počítač,* Vydavatelství a nakladatelství: Grada Publishing, a.s., Praha 7, 2015, ISBN s. 28-32 978-80-247-5453-6
[72] E-bezpečí, *Jak zabezpečit počítač,* [online]. [cit. 2022-3-13]. Dostupné z WWW: https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1653-jak-zabezpecit-pocitac
[73] Letem světem applem, *Kompletní návod na zabezpečení vašich internetových účtů,* [online]. [cit. 2022-3-13]. Dostupné z WWW: https://www.letemsvetemapplem.eu/2020/01/01/kompletni-navod-na-zabezpeceni-vasich-internetovych-uctu/

přílohu ta do našeho počítače nainstaluje program pro vzdálený přístup k počítači Remote Administration Tools, tak má možnost útočník kameru na dálku ovládat a zjistí tak jestli kamera je aktivní. Hackeři využívají pro útoky škodlivé programy, kde se dostanou do notebooku a můžou tak nahrát intimní záběry majitelů, kterým potom zašlou email s výhružným dopisem, jestli jim nepošlou určitou částku jinak tyto záběry zveřejní na sociálních sítích nebo jejich kolegům do práce. Policie upozorňuje uživatelům, aby na email nereagovali a smazali email, označili za spam.[74]

[74] E-bezpečí, *Jak zabezpečit počítač,* [online]. [cit. 2022-3-13]. Dostupné z WWW: https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1653-jak-zabezpecit-pocitac

8 Empirická část – kvalitativní výzkumné šetření

V praktické části bylo cílem zjistit, jestli uživatelé mají zkušenost o zneužití jejich identity, osobních údajů na internetu, sociálních aplikacích a jaké používají zabezpečení proti počítačové kriminalitě. Bylo osloveno 50 respondentů prostřednictvím elektronického dotazování my.survio.com, celý dotazník lze prohlédnout zde.[75]

8.1 Plán výzkumu

Pro získání dat jsem zvolil elektronické dotazování, který obsahuje 20 otázek, trvá 3-5 minut je bezčasově omezený a anonymní. Použil jsem jednoduché otázky, aby respondenti je dobře pochopili a mohli dotazník vyplnit.

Dotazník obsahoval následující otázky:

1. Váš věk?
2. Vaše Pohlaví?
3. Setkali jste se s počítačovou kriminalitou?
4. Myslíte si, že zneužívání identity je v dnešní době časté?
5. Jaké znáte rizika zneužití identity?
6. Zneužil někdo Vaše osobní informace z počítače nebo mobilu? Např. (fotky, zprávy, videa, dokumenty)
7. Setkali jste se s vyhrožováním na internetu přes sociální sít?
8. Pokoušel se vám někdo dostat k Vaší kreditní kartě, prostřednictvím hackingu?
9. Byl Vám někdy odcizen internetový bankovní účet?
10. Komunikovali jste s někým, kdo se vydával za někoho jiného a vy jste o tom vůbec nevěděli?
11. Používáte sociální sítě?
12. Jaké sociální sítě používáte?
13. Byl Vám odcizen uživatelský účet na sociálních sítí?
14. Máte nastavený veřejný nebo soukromí profil na Facebooku a Instagramu?
15. Používáte víceúrovňové zabezpečení Vašeho počítače nebo telefonu
16. Používáte antivirový program na Vaši výpočetní techniku?
17. Používáte šifrování pevných disků a přenositelných disků ve Vašem počítači?

[75] My.survio.com [online]. *Počítačová kriminalita zaměřena na zneužití identity a trestná činnost s tím spojená.* [cit. 2022-3-19]. Dostupné z WWW:https://www.survio.com/survey/d/V9W4F4Q7Z8K6N8U1B

18. Máte zabezpečenou Vaši domácí síť?
19. Myslíte si, že prevence počítačové kriminality je důležitá pro bezpečnost na internetu?
20. Jaké znáte preventivní programy?

Pomocí dotazníkové šetření jsem chtěl zjistit, jestli respondenti mají povědomí o počítačové kriminalitě a zneužití identity, jakou mají s ní zkušenost či jestli používají zabezpečení ve své výpočetní technice a uživatelských účtů.

8.2 Vyhodnocení získaných dat

Po získání dat z elektronického dotazníku jsem data zpracoval v programu Microsoft Office Excel. Grafy obsahují otázku, která byla položena respondentům v dotazníkovém šetřením a výsledky odpovědí. Stručně zhodnotím odpovědi respondentů s krátkým závěrem pod každým grafem.

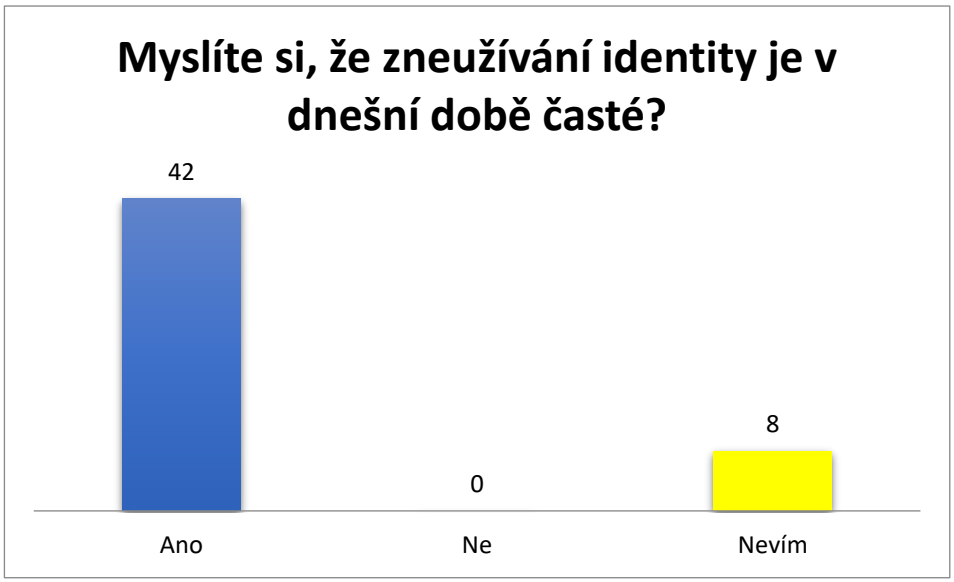
Osloveni byli respondenti od sedmnácti let do osmdesáti let, průměrný věk respondentů byl 36 let. Dotazník vyplnilo 28 mužů a 22 žen.

Graf č. 1 – pojem počítačová kriminalita[76]

Graf č. 1 byl zaměřen, jestli respondenti se setkali někdy s počítačovou kriminalitou z 50 odpovědí 26 respondentů mělo zkušenost s počítačovou kriminalitou a zbylých 24 nemají žádnou zkušenost a zatím se s ní vůbec nesetkali.

[76] Vlastní zdroj

Graf č. 2 – zneužívání identity [77]



Graf č. 2 znázorňuje kolik respondentů si myslí, že zneužívání identity se stává častým trestným činem. Většina lidí si uvědomuje, že útoky na zneužití identity jsou nebezpečné a vyskytují se mnohem častěji, protože s útokem na identitu se můžou setkat kdekoliv na internetu. Zbylých 8 respondentů si nejsou jistí, jestli útoky na identitu jsou v dnešní době tak časté. S tímto vyhodnocením jsem spokojený, protože většina lidí si myslí, jak je nebezpečné zneužívání identity a mají představu, že tato trestná činnost se objevuje ve vysoké míře v dnešní době.

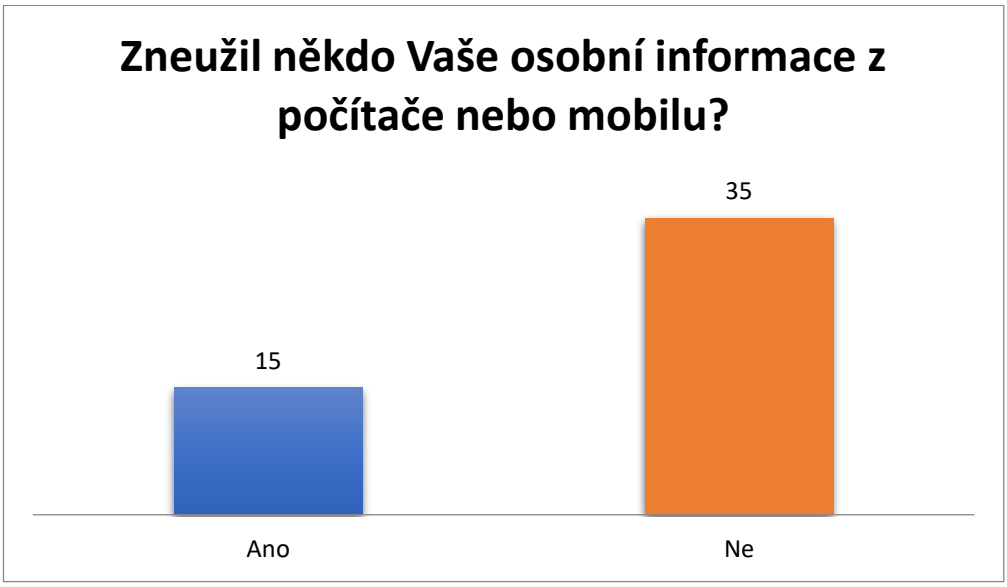
[77] Vlastní zdroj

Graf č. 3 – rizika zneužití identity[78]

Graf č. 3 ukazuje kolik respondentů rozumí těmto pojmů rizik ke zneužití identity. Většina respondentů zná riziko kyberstalking, 20 respondentů má povědomí o sociálním inženýrství a zbylých 14 respondentů o kybergroomingu. Tento výsledek jsem čekal, že většina lidí bude znát hlavně riziko kyberstalking, protože každý má dneska webkameru v notebooku či mobilu, které využívají ke komunikaci s lidmi, hlavně v období koronavirusu, kde přes kamerové zařízení to bylo nejdůležitější spojení jak s prací, tak i se školou.

[78] Vlastní zdroj

Graf č. 4 – zneužití informací z počítače nebo mobilu[79]



Graf č. 4 znázorňuje kolik respondentů bylo zneužito jejich osobní informace přes počítač či mobilní zařízení. Tento hlavně graf poukazuje, jak si respondenti chrání své osobní informace, protože 15 respondentům bylo zneužito jejich osobní informace z výpočetní techniky, což vyplívá že nemají dobře zabezpečenou svoji výpočetní techniku, nebo si nedávají pozor a své informace zveřejňují na sociálních sítích, které nemají taky zabezpečené. Na druhou stranu většina lidí celkem 35 nezneužil žádný útočník jejich osobní informace, protože nejspíš si dávají pozor a pečlivě si svoje informace chrání a zabezpečují si svoji výpočetní techniku a domácí síť, mají představu, že by jim někdo mohl jejich informace zneužít.

[79] Vlastní zdroj

Graf č. 5 – vyhrožování přes sociální síť[80]

Graf č. 5 ukazuje kolik respondentům bylo vyhrožováno přes sociální sít. Většina respondentů se nesetkala s vyhrožováním na sociální síti, zatím co 22 z 50 respondentů se setkalo s vyhrožováním prostřednictvím sociální sítě. Výsledek ukazuje, že vyhrožování na sociálních sítích je častým jevem.

[80] Vlastní zdroj

Graf č. 6 – pokus o získání kreditní karty prostřednictvím hackingu[81]

Graf č. 6 znázorňuje, jestli dotazovaný lidi, kteří používají internetové bankovnictví, někdo pokoušel dostat prostřednictvím metody počítačové kriminality hackingu. Většina respondentů, která odpověděla ne se jim nikdo nedostal k jejich kreditní kartě, ale 9 respondentům se útočník pokoušel dostat prostřednictvím hackingu k jejich kreditní kartě, takže tento jev je pořád aktuální a dobré mít stále dobře zabezpečenou kreditní kartu. Posledních 13 respondentů vůbec netuší jestli, jim někdo se pokoušel dostat do kreditní karty.

[81] Vlastní zdroj

Graf č. 7 – odcizení bankovního účtu[82]

Graf č. 7 je zaměřený kolik lidem bylo odcizeno internetový bankovní účet. Skoro všem respondentům se nikdy nestalo, že by jim někdo odcizil internetové bankovnictví, ale jenom 2 z 50 respondentům ano. Myslím si, že většina lidí si dává pozor a silně si zabezpečuje své bankovní účty, hlavně na internetu a používá dobrou bankovní službu přes internet, protože zná riziko odcizení peněz prostřednictvím počítače, ale ti zbylí respondenti, buď nepoužívají silné zabezpečení svého internetového bankovnictví a podceňují silnou ochranu bezpeční svých peněz. Odcizení internetového bankovnictví je stále na běžném pořádku, ale je na nás, jak budeme mít zabezpečený účet.

[82] Vlastní zdroj

Graf č. 8 – komunikace kdo se vydával za někoho jiného[83]

Graf č. 8 znázorňuje kolik respondentům se stalo, že komunikovali s osobou, která se vydávala za někoho jiného, a oni vůbec nevěděli, kdo se skrýval za něčí identitou. Výsledek mě překvapil, protože 21 respondentů komunikovalo s někým úplně jiným, než si oni mysleli a 21 respondentů nekomunikovali a zbylých 8 nemají vůbec tušení. Dost často se vyskytují útočníci, kteří použijí cizí informace a fotky někoho jiného, aby komunikovali se svou potencionální obětí a pokusili se navázat kontakt se svoji potencionální obětí a 21 lidí z 50 dotázaných je velké číslo a tento jev se vyskytuje často, proto by si měli lidi dávat pozor s kým jsou v kontaktu hlavně s cizím člověkem, kterého vůbec neznají.

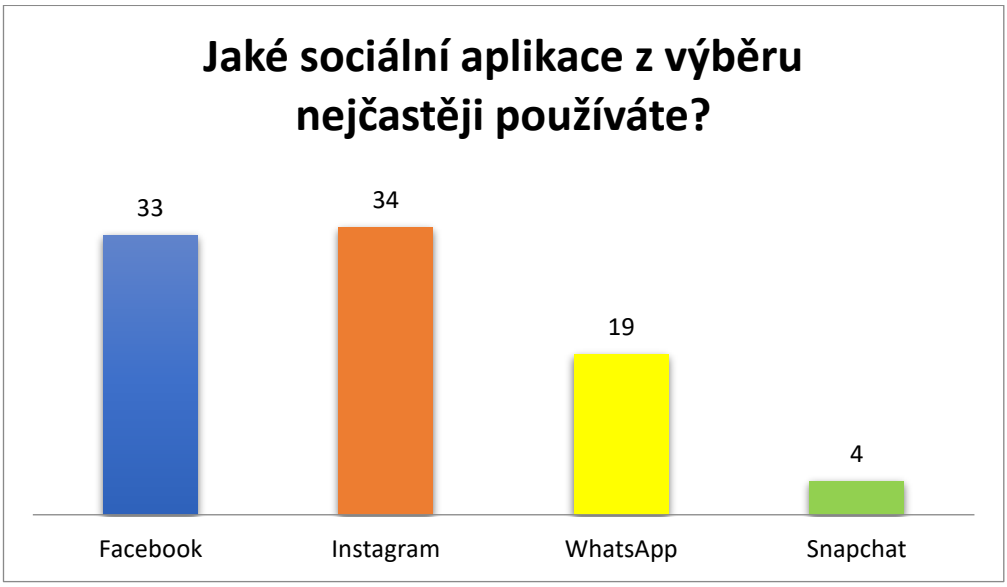
[83] Vlastní zdroj

Graf č. 9 – používání sociálních sítí[84]

Graf č. 9 byl určen k tomu kolik lidí používá sociální sítě, 46 respondentů z 50 sociální sítě používají a zbylé 4 respondenti vůbec. Výsledek ukazuje, že obrovská většina sociální sítě používá, hlavně ke komunikaci.

[84] Vlastní zdroj

Graf č. 10 – sociální aplikace[85]



Graf č. 10 ukazuje jakou sociální síť nejvíc používají respondenti. Vyrovnané výsledky jsou u sociální sítě Facebook a Instagram, kde u první sociální sítě používá 33 respondentů z 50 a u druhé sociální sítě 34 respondentů z 50. Většina respondentů, která používají Facebook tak zároveň používají i Instagram, protože je to od stejného majitele Marka Zuckerberga. Sociální síť WhatsApp není zas tak populární, protože to používá jen 19 respondentů a sociální síť Snapchat jen 4 respondenti, což vyplívá z toho, že Snapchat už je mrtvá sociální síť, kterou moc lidí nebaví. Nejoblíbenější sociální síť jsou Facebook a Instagram, kterou nemají žádnou silnou konkurenci.

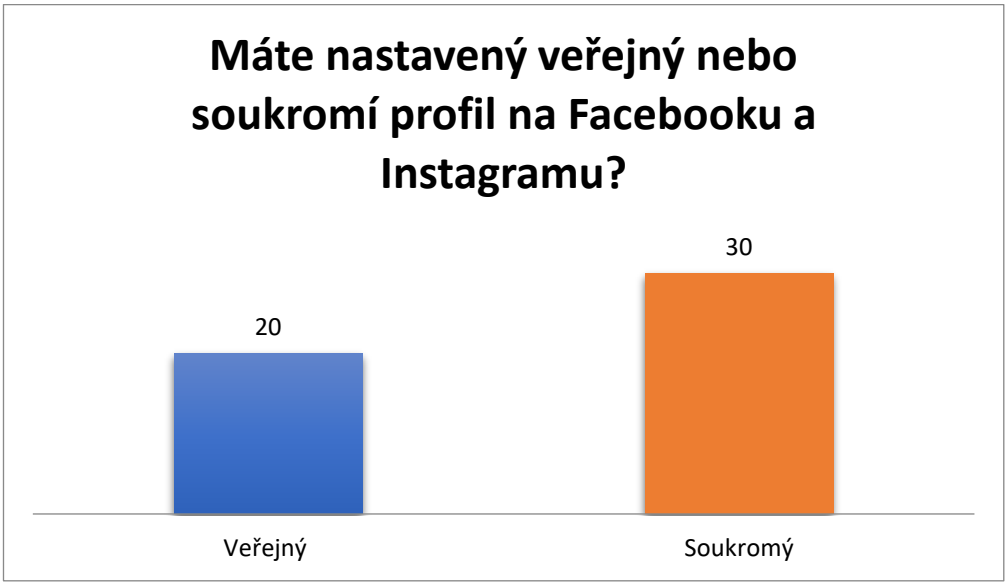
[85] Vlastní zdroj

Graf č. 11 – odcizení uživatelského účtu na sociálních síti[86]

Graf č. 11 znázorňuje kolik respondentů dotázaných byl odcizen uživatelský účet na sociální síti, jako je například Facebook nebo Instagram, kde je více uživatelů podle mého dotazníkového šetření z grafu č 8. Většině respondentů nikdy nebyl odcizen uživatelský účet, ale 15 respondentů z 50 ano. Myslím si že odcizení uživatelského účtu je časté, ale jen pokud když uživatelský účet není dostatečně zabezpečený silným heslem a dvoufázovým ověřením.

[86] Vlastní zdroj

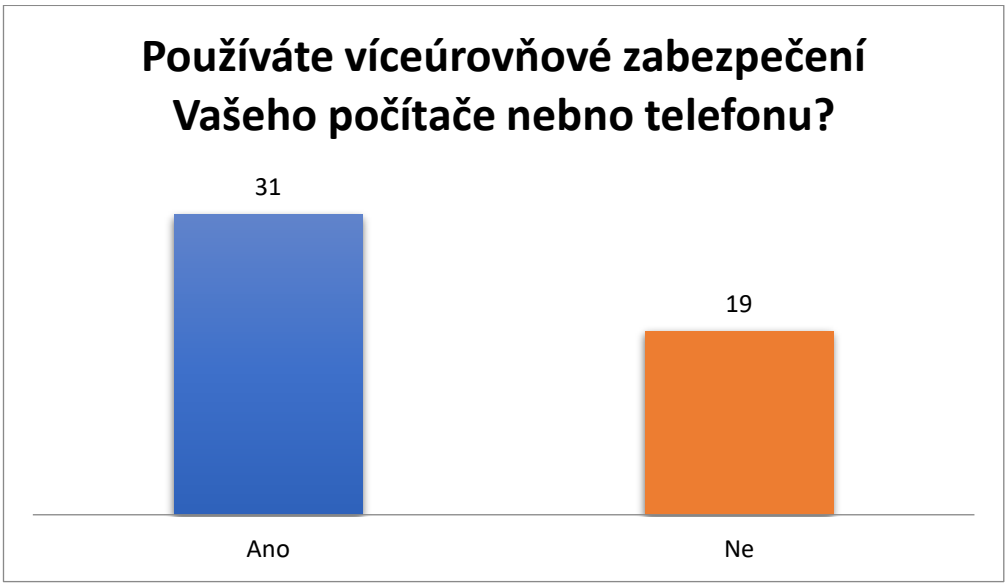
Graf č. 12 – nastavení soukromého nebo veřejného profilu na Facebooku a Instagramu[87]



Graf č. 12 znázorňuje kolik lidí má nastavený veřejný nebo soukromý profil na Facebooku a Instagramu. Nastavený soukromý profil má 30 respondentů z 50, protože se obávají, že by jim cizí člověk mohl koukat na jejich profil, ukládat si fotky, psát jim zprávy, komentovat příspěvky. Nastavení soukromého profilu je výborná věc, protože si lidi chrání svůj profil a zároveň oni rozhodují a tom kdo bude sledovat jejich profil, jako třeba jejich přátelé a rodina. Veřejný profil má nastaveno zbylých 20 respondentů, nejspíš jim nevadí, že jejich fotky a informace na jejich profilu může vidět úplně každý člověk, který klikne na jejich profil a můžou hned jim napsat třeba výhružnou zprávu a ukládat si jejich fotky atd. Jsem spokojený, že většina používá nastavení soukromého profilu pro jejich bezpečí a soukromí.

[87] Vlastní zdroj

Graf č. 13 – používání víceúrovňového zabezpečení počítače nebo telefonu[88]



Graf č. 13 ukazuje kolik respondentů dotázaných používá víceúrovňové zařízení jejich výpočetní techniky 31 z 50 dotázaných používá víceúrovňové zabezpečení jejich výpočetní techniky, protože chtějí mít svoji techniku zabezpečenou a svoje informace a vědí, že může nastat riziko, že by chtěl jejich informace někdo získat. Zbytek respondentů odpovědělo, že nemají víceúrovňové zabezpečení a riskují svůj počítač a telefon k riziku, který může nastat jako třeba útok přes metodu hacking.

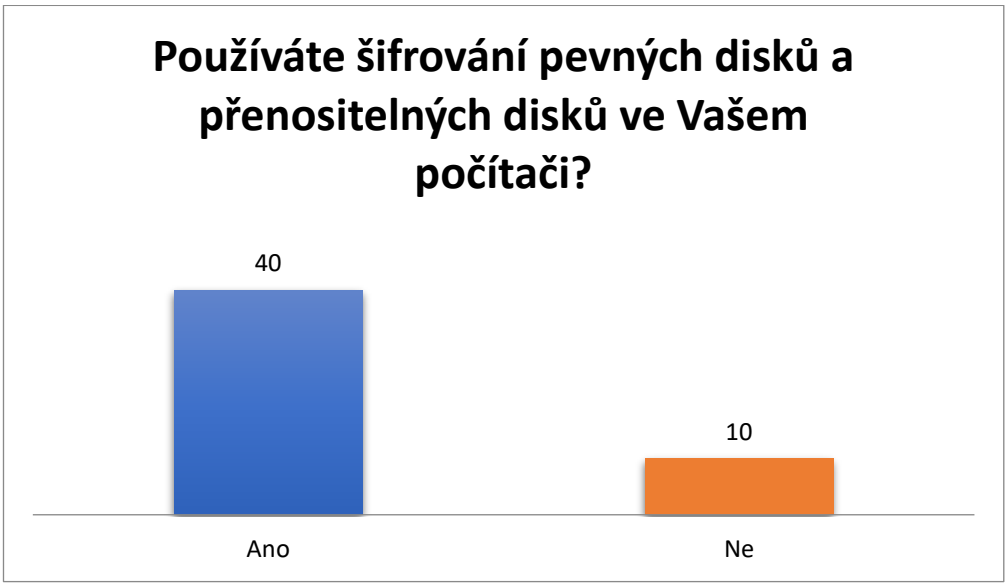
[88] Vlastní zdroj

Graf č. 14 – používání antivirového programu[89]

Graf č. 14 znázorňuje kolik respondentů používá antivirový program pro jejich výpočetní techniku, většina dotázaných respondentů 38 z 50 používá antivirový program a chrání svoji výpočetní techniku před škodlivými viry, malwerem nebo před samotným vniknutím do počítače. Překvapilo mě, že zbytek 12 respondentů, kteří odpověděli, že nepoužívají antivirový program pro jejich ochranu počítače. Myslím si, že nevědí o rizikách, které můžou nastat, když si nebudou chránit svůj počítač antivirovým programem a podceňují tím ochranu svých informací a útočníkům dávají přímou pozvánku do jejich systému.

[89] Vlastní zdroj

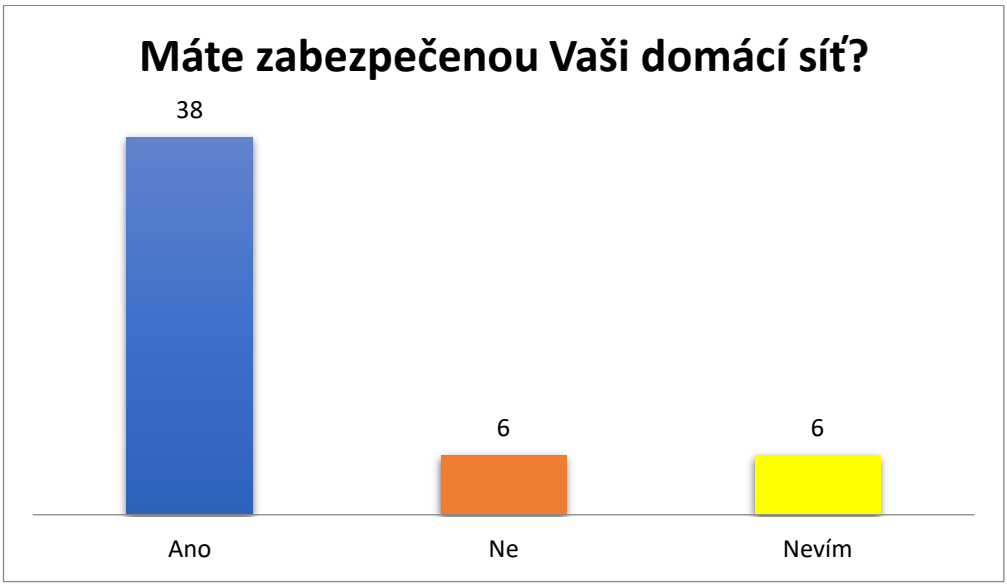
Graf č. 15 – používání šifrování pevných disků a přenositelných disků v počítači[90]



Graf č. 15 je zaměřený na používání šifrování pevných disků a přenositelných disků v počítači. Většina dotázaných respondentů používá šifrování pevných a přenositelných disků a chrání svoje data, ale zbylých 10 vůbec a vystaví svoje disky a počítač k nebezpečnému riziku.

[90] Vlastní zdroj

Graf č. 16 – zabezpečená domácí síť[91]



Graf č. 16 ukazuje kolik lidí má zabezpečenou svoji domácí síť. Jsem mile překvapený, že většina respondentů má svoji domácí síť zabezpečenou chrání si tím svá data a vědí o možném nebezpečném riziku, který by mohl nastat, kdyby vůbec neměli zabezpečenou domácí síť. Zbylých 6 respondentů, kteří odpověděli, že nemají zabezpečenou svoji domácí síť nejsou nejspíš seznámeni s možným nebezpečným rizikem a svoje informace a data nechávají volným způsobem útočníkům. A zbytek dotázaných vůbec netuší.

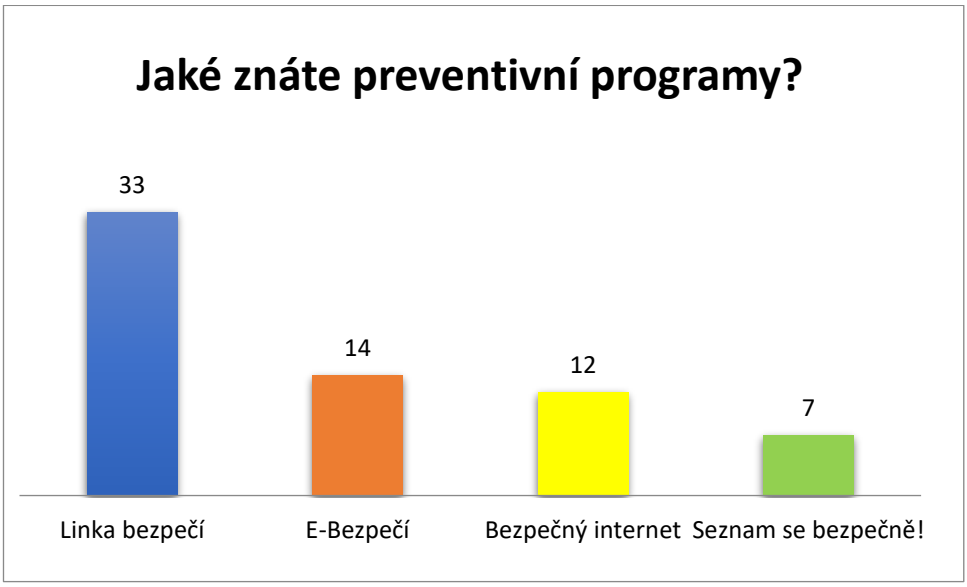
[91] Vlastní zdroj

Graf č. 17 – důležitost prevence kriminality pro bezpečí na internetu[92]

Graf č. 17 znázorňuje kolik respondentů si myslí, že prevence počítačové kriminality je důležitá pro bezpečnost na internetu 47 z 50 dotázaných odpovědělo ano, protože si myslí, že prevence je počítačové kriminality je velmi důležitá 2 respondenti odpověděli, že není nejspíš nemají tolik informací o prevenci kriminality, a proto si to nemyslí a poslední respondent odpověděl, že vůbec netuší, jestli je prevence kriminality důležitá pro bezpečnost na internetu.

[92] Vlastní zdroj

Graf č. 18 – preventivní programy[93]



Graf č. 18 ukazuje kolik dotázaných respondentů zná preventivní program a o jakých preventivních programech slyšel. Většina respondentů zná program Linka bezpečí, 14 respondentů odpovědělo E-bezpečí, 12 Bezpečný internet a zbylých 7 Seznam se bezpečně!. Lidi mají povědomí o preventivních programech, které jsou důležité s bojí počítačovou kriminalitou a pomáhají lidem proti útokům ve virtuálním světě a jak se nejlépe bránit.

[93] Vlastní zdroj

Závěr

Počítačová kriminalita se stala novým fenoménem moderní doby, protože výpočetní technologie se zdokonalují a zahlcují celou společnost, která víc žije ve virtuálním světě, a vznikají nové formy trestných činností počítačové kriminality, která nabírá na rychlosti a jiných metodách, které pachatelé vytvářejí, využívají počítač, internetovou síť jako prostředník k poškození, zneužití, krádež k obohacení ve svůj prospěch. Cílem této práce bylo charakterizovat, co znamená počítačová kriminalita a zneužití identity, jaké trestné činnosti s tím jsou spojeny. Při vypracování práce bylo vycházeno z literárních, internetových a legislativních dokumentů.

Práce se skládá z několika kapitol, které charakterizují danou tematickou problematiku, kde na začátku je popsána historie, základní pojmosloví a východisek druhů počítačové kriminality. Kapitola čtvrtá Zneužití a krádež identity je hlavním tématem této práce, protože naše identifikační údaje, hesla, PIN kódy, uživatelské účty jsou naší virtuální totožností a provádíme s nimi každý den určité operace v různých institucích, jako jsou pojišťovny, banky, nemocnice či finanční úřady. Odcizení a zneužití našich identifikačních údajů apod. nám může těžce znepříjemnit náš pohodový život, který si vytváříme podle našich představ a cílů. V kapitole je popsána, jaké metody pachatel používá ke zneužití identity a krádeži informací jako například metoda sociální inženýrství nebo kybergrooming, kapitola také obsahuje, jak pachatel si vytváří falešnou identitu na sociálních sítích a jakým způsobem oslovuje svoje potencionální oběti, kde jsem vymezil pár příkladů zaslaných zpráv.

Pátá kapitola se zaměřuje na problematiku sociální sítě, kde jsou popsány, jak fungují na náš mozek a proč jsou takovým spalovačem našeho času, ale zároveň je zde popsáno k čemu slouží. Sociální sítě nesou s sebou rizika v podobě kyberšikany, sextingu či kyberstalkingu a jakou mají právní kvalifikaci kromě kyberšikany, protože právní úpravu český zákoník nezná.

Šestá kapitola se věnuje viktimologickým aspektům počítačové kriminality, jsou zde informace o pojmech viktimizace, viktimnost a vysvětlena důležitost viktimologické prevence, která má zajistit včasnou obranu před možnými nepříjemnými následky. Prevence počítačové kriminality má v České republice několik preventivních programů například Seznam se bezpečně!, E-bezpečí, Bezpečný internet na které

se člověk může obrátit, přečíst potřebné informace jak se bránit před útokem pachatele a na co si dát pozor na internetu.

Závěrečná kapitola teoretické části se zabývá bezpečnostními opatřeními, zde je demonstrováno, proč je ochrana naší výpočetní techniky velmi zásadní. Důležitost antivirových programů, vytváření silných hesel, nastavení bezpečnosti domácí sítě a aplikací, uživatelských účtů či webové kamery na notebooku nebo mobilního telefonu.

Empirická část práce, která je vymezena v osmé kapitole, kde je použita metoda dotazníkového šetření oslovených respondentů. Úkolem bylo zjištění, jaké mají znalosti a zkušenost s počítačovou kriminalitou o zneužití identity, osobních údajů, krádeže účtů, jaké používají zabezpečení. Podle informací bylo zjištěno, že většina oslovených respondentů má povědomí o počítačové kriminalitě, jaké rizika má ale také výsledky ukázali, že se setkali s vyhrožováním přes sociální sítě, odcizení uživatelského účtu a dost respondentů mělo zkušenost s komunikací s člověkem, který se vydával za někoho jiného. V rámci dílčích a zevšeobecňujících výstupů užitého výzkumného šetření lze pozitivně konstatovat empiricky zjištěnou skutečnost, kdy respondenti využívají dobré zabezpečení své výpočetní techniky a uživatelských účtů. Avšak v menší míře někteří respondenti svou ochranu podceňují a nemají předtuchu, jakému riziku vystavují svá nezabezpečená osobní data, které může útočník jednoduše využít například k páchaní trestné činnosti.

Seznam použitých zdrojů

Literární zdroje

1. ADAMETZ, Otto a kolektiv autorů, *Kriminalistická problematika při odhalování, vyšetřování a prevenci počítačové kriminality.* Vydavatelství a nakladatelství: Policejní akademie České republiky, Praha, 1997, 204 s. ISBN 80-85981-50-5

2. BÍMOVÁ, Alena, *Počítačová kriminalita a naše doba*. Praha: IDG Czechoslovakia, a.s., 1990, 125 s. ISBN 80-900872-2-1

3. ECKERTOVÁ, Lenka, DOČEKAL, Daniel, *Bezpečnost dětí na internetu.* Computer Press, Brno, 2013, Albatros Media a. s., Na Pankráci 30, Praha 4, 224 s. ISBN 978-80-251-3804-5

4. JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech, a trojských koních bez tajemství*. Grad, Praha, 2007, 284 s. ISBN 9788024715612-8024715619

5. KOLEKTIV AUTORŮ, *Počítačová kriminalita ochrana výpočetní techniky a dat.* RINGO, Praha 6, v gesci Československé společnosti pro kriminalistiku a Akademie J.A Komenského ČR, 1991, 182 s. ISBN 80-900634-0-3

6. KRÁL, Mojmír. Bezpečný internet: Chraňte sebe i svůj počítač, Vydavatelství a nakladatelství: Grada Publishing, a. s., Praha 7, 2015, 184 s. ISBN 978-80-247-5453-6

7. KOŽÍŠEK, Martin, PÍSECKÝ Václav. *Bezpečně na internetu průvodce chováním ve světě online*. Grada Publishing, a. s., U Průhonu 22, Praha 7, 2016, 176 s. ISBN 978-80-247-5595-3

8. TOMÁŠE, Jan. *ÚVOD DO KRIMINOLOGIE,* Grada Publishing, a.s., U Průlomu 22, 170 00 Praha 7, 214 s. ISBN 978-80-247-2982-4

9. PORADA, Viktor, KONDRÁD, Zdeněk. *Metodika vyšetřování počítačové kriminality.* Policejní akademie České republiky, Praha 1997, 54 s. ISBN 80-85981-75-0

10. ROGERS, Vanessa. *Cyberbullying, Activities to Help Childern and Teens to Stay Safe in a Texitnt, Twittering, Social Networking World.* Jessica Kingsley Publisher, London, 2010, 128 p. ISB 978-80-7367-984-2

11. ŠALMON, Tomáš. *(Ne)bezpečný internet,* Albatros Media a. s., 2021 292 s.

12. ŠEVČÍKOVÁ, Anna, *Děti a dospívající online,* Grada Publishing, a. s., U Průhonu 22, Praha 7, 184 s., 978-80-247-5010-1

13. VELIKOVSKÁ, *Martina. Psychologie obětí trestných činů,* Vydavatelství a nakladatelství: Grada Publishing, a.s. U průhonu 22, 170 00 Praha 7, 2016, 168 s. ISBN 978-80-271-9172-7

14. VITOUŠOVÁ, Petra. *Pomoc obětem (a svědkům) trestných činů-Příručka pro pomáhající profese,* Grada Punlishing a.s., 2007, 191 s. ISBN 8024720140, 9788024720142

15. VLČEK, Martin, *Počítače a kriminalita*. Praha: Academia. Nakladatelství Československé akademie věd, 1989, 96 s. ISBN 80-200-01

Elektronické zdroje

1. BDO Česká republika*, Metody sociálního inženýrství*. [online]. [cit. 2021-11-3]. Dostupné z WWW: https://www.bdo.cz/cs-cz/blog/it-security/brezen-2021/metody-socialniho-inzenyrstvi

2. Bezpečný Internet, *Krádež Identity.* [online]. [cit 2021-10-12]. Dostupné z WWW: http://www.bezpecnyinternet.cz/pokrocily/ochrana-prav/kradez-identity.aspx

3. E-bezpečí, *Jak zabezpečit počítačovou síť,* [online]. [cit. 2022-3-13]. Dostupné z WWW: *https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1651-jak-zabezpecit-domaci-pocitacovou-sit*

4. E-bezpečí, *Případy kybergroomingu I.,* [online vydání 2009-2-15], [cit. 2022-2-10]. Dostupné z WWW:https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kybergrooming/33-112

5. E-bezpečí, *Případy kybergroomingu I.*, [vid. 14.2.2009]. [cit. 2022-1-4]. *Rizikové jevy kybergroomingu*. Dostupné WWW:https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kybergrooming/33-112

6. E-bezpečí, *Případy kybergroomingu I.,* [online vydání 2009-2-15], [cit. 2022-2-10]. Dostupné z WWW:https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kybergrooming/33-112

7. Internetem bezpečně, *Krádež identity*. [online]. [cit. 2021-10-12]. Dostupné z WWW: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/kradez-identity/

8. Internetem bezpečně, *Sexting,* [online]. [cit. 2022-3-11]. Dostupné z WWW: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/sexting/

9. Internetem bezpečně, *Sexting,* [online]. [cit. 2022-3-11]. Dostupné z WWW: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/sexting/

10. Jak se Rychle Naučit, *Nebezpečí sociálních sítích, které si neuvědomujete,* [online]. [cit. 2022-3-11]. Dostupné z https://jakserychlenaucit.cz/nebezpeci-socialnich-siti/

11. Letem světem applem, *Kompletní návod na zabezpečení vašich internetových účtů,* [online]. [cit. 2022-3-13]. Dostupné z WWW: https://www.letemsvetemapplem.eu/2020/01/01/kompletni-navod-na-zabezpeceni-vasich-internetovych-uctu/

12. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, *O významu poznávání obětí trestné činnosti,* [online]. [cit. 2022-4-11]. Dostupné z WWW: https://www.mvcr.cz/clanek/o-vyznamu-poznavani-obeti-trestne-cinnosti.aspx

13. Nebojte se internetu*, Sociální sítě.* [online]. [cit. 2022-2-11]. Dostupné z WWW: https://www.nebojteseinternetu.cz/page/3396/socialni-site/

14. POLICIE ČESKÉ REPUBLIKY, *Majetkové trestné činy*. [online]. [cit. 2021-10-10]. Dostupné z WWW: https://www.policie.cz/clanek/pomoc-obetem-tc-majetkove-trestne-ciny.aspx

15. POLICIE ČESKÉ REPUBLIKY*, Ztráta Identity.* [online]. [cit. 2021-10-12]. Dostupné z WWW: https://www.policie.cz/clanek/ztrata-identity.aspx

16. TOPRANKER.CZ. *Co je to WWW (word wibe web)?* [online]. [cit. 2021-10-8]. Dostupné z WWW: https://topranker.cz/slovnik/www-world-wide-web/

17. Top security, *Průmyslová špionáž se týká malých i velkých firem. Jak se bránit?* [online]. [cit. 2021-11-5]. Dostupné z WWW: https://www.topsecurity.cz/blog/clanek/prumyslova-spionaz-se-tyka-malych-i-velkych-firem-jak-se-branit

18. VNOUČEK, Petr. *Facebookový vrah na doživotí.* Webový portál Týden.cz. [online vydání 2010-3-10] [cit. 2022-2-12]. Dostupné z WWW: https://www.theguardian.com/uk/2010/mar/09/merseyside-police-peter-chapman-facebook

19. Wikisofia, *Cyberstaling,* [online]. [cit. 2022-3-11]. Dostupné z WWW: https://wikisofia.cz/wiki/Cyberstalking

Legislativní dokumenty

1. ŠÁMAL, Pavel, *Trestní zákoník: komentář. 2.* Vydavatelství a nakladatelství: C.H. Beck, Praha, 2012, 258 s. ISBN 978-80-7400-428-5

2. ČESKO. Zákon č. 40/2009 Sb., Trestní zákoník, § 209 Podvod, [online]. In *Sbírka zákonů, Česká republika.* 2009, částka 2. Dostupné z WWW: https://www.zakonyprolidi.cz/cs/2009-40?text=209

3. ČESKO. Zákon č. 40/2009 Sb., Trestní zákoník, § 206 Zpronevěra, [online]. In *Sbírka zákonů. Česká republika.* 2009, částka 2. Dostupné z WWW: https://www.zakonyprolidi.cz/cs/2009-40?text=206

4. ČESKO. Zákon č. 40/2009 Sb. Trestní zákoník, §205 Krádež. [online]. In *Sbírka zákonů, Česká republika.* 2009, částka 2. Dostupné z WWW: https://www.zakonyprolidi.cz/cs/2009-40?text=205

5. ČESKO. Zákon č. 40/2009 Sb. Trestní zákoník, §232 Poškození záznamu v počítačovém systému a na nosiči a zásah do vybavení počítače z nedbalosti. [online]. In *Sbírka zákonů, Česká republika.* 2009, částka 2. Dostupné z WWW: https://www.zakonyprolidi.cz/cs/2009-40?text=232

6. ČESKO. Zákon č. 40/2009 Sb., Trestní zákoník, § 182–232. [online]. In *Sbírka zákonů, Česká republika,* 2009 částka 2. Dostupné z WWW: http://zakony.centrum.cz/trestni-zakonik/cast-2-hlava-2-dil-2

Seznam zkratek

atd.	a tak dále
apod.	a podobně
FBI	Federal Bureau of Investigation
ICI	Firm Imperial Chemical Industies
MŠMT	Ministerstvo školství, mládeže a tělovýchovy
MVČR	Miniaterstvo vnitra České republiky
PIN	Personal Identification Number
SMS	Short Message Service
tj.	to je
Tzv.	takzvaný
WWW	World Wide Web

Seznam tabulek a grafů

Přílohy

Dotazník

Vážené respondetky, vážení respondenti,

Obracím se na Vás s žádostí o vyplnění mého dotazníku, který poslouží jako podklad pro Bakalářskou práci na téma počítačová kriminalita zaměřena na zneužití identity a trestná činnost s tím spojená. Účast ve výzkumu je anonymní.

Předem děkuji za spolupráci,

Adam Struhovský

Student 3. Ročníku Bezpečnostně právní činnosti Vysoké školy evropských a regionálních studií

1. **Váš věk?**

   Napište číslovkou nebo slovy

2. **Vaše Pohlaví?**

Muž

Žena

3. **Setkali jste se s počítačovou kriminalitou?**

Ano

Ne

4. **Myslíte si, že zneužívání identity je v dnešní době časté?**

Ano

Ne

Nevím

5. **Jaké znáte rizika zneužití identity?**

Sociální inženýrství

Kybergrooming

Kyberstalikng

6. **Zneužil někdo Vaše osobní informace z počítače nebo mobilu? Např. (fotky, zprávy, videa, dokumenty)**

Ano

Ne

7. **Setkali jste se s vyhrožováním na internetu přes sociální sít?**

Ano

Ne

8. **Pokoušel se vám někdo dostat k Vaší kreditní kartě, prostřednictvím hackingu?**

Ano

Ne

Nevím

9. **Byl Vám někdy odcizen internetový bankovní účet?**

Ano

Ne

10. **Komunikovali jste s někým, kdo se vydával za někoho jiného a vy jste o tom vůbec nevěděli?**

Ano

Ne

Nevím

11. **Používáte sociální sítě?**

Ano

Ne

12. **Jaké sociální sítě používáte?**

Facebook

Instagram

Snapchat

WhatsApp

13. **Byl Vám odcizen uživatelský účet na sociálních sítí?**

Ano

Ne

14. **Máte nastavený veřejný nebo soukromí profil na Facebooku a Instagramu?**

Veřejný

Soukromý

15. **Používáte víceúrovňové zabezpečení Vašeho počítače nebo telefonu**

Ano

Ne

16. **Používáte antivirový program na Vaši výpočetní techniku?**

Ano

Ne

17. **Používáte šifrování pevných disků a přenositelných disků ve Vašem počítači?**

Ano

Ne

18. **Máte zabezpečenou Vaši domácí síť?**

Ano

Ne

Nevím

19. **Myslíte si, že prevence počítačové kriminality je důležitá pro bezpečnost na internetu?**

Ano

Ne

Nevím

20. **Jaké znáte preventivní programy?**

E-bezpečí

Seznam se bezpečně!

Bezpečný internet

Linka bezpečí