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

BAKALÁŘSKÁ PRÁCE

INTERNETOVÉ PODVODY A ROLE POLICIE ČESKÉ REPUBLIKY V INFORMOVÁNÍ VEŘEJNOSTI

Autor práce: Miroslav Šupík, DiS.
Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Vedoucí práce: JUDr. Milan Kocík, MBA, LL.M.
Katedra: Katedra právních oborů a bezpečnostních studií

2025

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 1632/5b, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Miroslav Šupík, DiS.
Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Internetové podvody a role Policie České republiky v informování veřejnosti

Název bakalářské práce v anglickém jazyce: Internet Fraud and the Role of the Police of the Czech Republic in Informing the Public

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, včetně titulů):
JUDr. Milan Kocík, MBA, LL.M.

Datum zadání bakalářské práce (měsíc, rok): listopad 2024

Cíl bakalářské práce:
Hlavním cílem bakalářské práce bude posoudit typy internetových podvodů a jejich četnost na území České republiky s důrazem na aktuální hrozby. Prvním vedlejším cílem bude zhodnotit efektivitu a metody informování veřejnosti o internetových podvodech ze strany Policie České republiky, včetně preventivních kampaní a dostupnosti informačních zdrojů. Druhým vedlejším cílem bude navrhnout doporučení ke zlepšení informovanosti veřejnosti s cílem zvýšit povědomí o rizicích a prevenci internetových podvodů.

Student: Miroslav Šupík, DiS.	29.11.2024 *datum*	*podpis*
Vedoucí práce: JUDr. Milan Kocík, MBA, LL.M.	29.11.2024 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	2.12.2024 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	9.12.2024 *datum*	*podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	10.12.2024 *datum*	*podpis*

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

Prohlašuji, že jsem bakalářskou práci vypracoval(a) 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.

.....

Rád bych poděkoval JUDr. Milanu Kocíkovi, MBA, LL.M. za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

ŠUPÍK, M. *Internetové podvody a role Policie České republiky v informování veřejnosti: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2025. 71 s. Vedoucí bakalářské práce: JUDr. Milan Kocík, MBA, LL.M.

Klíčová slova: internet, internetové podvody, kyberprostor, kybernetická trestná činnost, Policie České republiky, preventivní opatření, sociální sítě

Bakalářská práce se zabývá problematikou internetových podvodů, které představují jedno z největších nebezpečí v oblasti kybernetické bezpečnosti. V současné době se jedná o nejrozšířenější druh kybernetické trestné činnosti, která je zároveň potenciálním nebezpečím pro osoby všech věkových kategorií.

Hlavním cílem bakalářské práce bylo posoudit typy internetových podvodů a jejich četnost na území České republiky s důrazem na aktuální hrozby.

Prvním vedlejším cílem bylo zhodnotit efektivitu a metody informování veřejnosti o internetových podvodech ze strany Policie České republiky, včetně preventivních kampaní a dostupnosti informačních zdrojů.

Druhým vedlejším cílem bylo navrhnout doporučení ke zlepšení informovanosti veřejnosti s cílem zvýšit povědomí o rizicích a prevenci internetových podvodů.

ABSTRACT

ŠUPÍK, M. *Internet Fraud and the Role of the Police of the Czech Republic in Informing the Public*: *Bachelor's Thesis*. České Budějovice: The College of European and Regional Studies, 2025. 71 pgs. Supervisor: JUDr. Milan Kocík, MBA, LL.M.

Key words: internet, internet fraud, cyberspace, cybercrime, Police of the Czech Republic, preventive measures, social networks

The bachelor's thesis addresses the issue of internet fraud, which represents one of the greatest dangers in the field of cybersecurity. Currently, it is the most widespread type of cybercrime, posing a potential threat to people of all age groups.

The main objective of the bachelor's thesis was to assess the types of internet fraud and their frequency in the Czech Republic, with an emphasis on current threats.

The first secondary objective was to evaluate the effectiveness and methods of informing the public about internet fraud by the Police of the Czech Republic, including preventive campaigns and the availability of information resources.

The second secondary objective was to propose recommendations to improve public awareness in order to increase knowledge about the risks and prevention of internet fraud.

Obsah

Úvod

V současné době se nacházíme v období, které lze nazvat obdobím informačním. Dnes platí, že ten, kdo má přístup k informacím nebo ovládá nějaký informační systém a má odpovídající znalosti, má nezanedbatelnou výhodu. Tím, jak se stále stáváme více závislí na informačních technologiích, se také zároveň stáváme ohroženější z hlediska kybernetické bezpečnosti.[1]

Kybernetická trestná činnost, často označována také jako kyberkriminalita, se v posledních letech stala velkým problémem nejen pro seniory, ale také pro osoby všech věkových kategorií. Nejen v České republice, ale i za našimi hranicemi, se kyberkriminalita stala problémem, který má potenciál do budoucna spíše narůstat než naopak. Ke kyberkriminalitě dochází čím dál častěji a může nám způsobit značnou škodu. Řadí se tak k těm nejzávažnějším rizikům dnešní doby. Její velká nebezpečnost pro společnost spočívá především v tom, že náklady na její realizaci jsou s ohledem na způsobenou škodu zanedbatelné.[2] V posledních letech prošla velkým rozvojem a v současné době se jedná o jednu z nejvíce sofistikovaných trestných činností. Je to dáno zejména tím, že pachatelům kyberkriminality dnešní moderní technologie velmi usnadňují práci. Pachatelé mohou v rámci svého protiprávního jednání naráz oslovit velké množství potenciálních obětí. Sofistikovanost a kvantita této trestné činnosti jsou nyní na takové úrovni, že se s ní můžeme setkat úplně všichni, bez ohledu na to, zda jsme aktivními uživateli internetu a sociálních sítí či nikoliv.

Velké riziko představuje v dnešní době také závislost na internetu a sociálních sítích. V historii jsme se již přesvědčili o tom, že nové technologie a jejich význam není jednoduché předvídat. Spousta zdánlivě zajímavých technologií po čase začaly stagnovat, a některé se postupem času úplně vytratily.[3] Podobný osud však ani internet a ani sociální sítě nepotká. Ty se budou s postupem času neustále vyvíjet. I tento fakt může mít velký vliv na to, že do prostředí internetu a sociálních sítí pronikají stále mladší a mladší osoby, které mnohdy neví, jak se mají v tomto prostředí s ohledem na vlastní bezpečí chovat. V dnešní době se již děti s internetem neseznamují poprvé při hodinách informatiky, ale

[1] ŠULC, V. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018. s. 5.
[2] Tamtéž, s. 26.
[3] MATEJKA, J. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praha: CZ.NIC, 2013. s. 28.

doma na mobilním telefonu či tabletu, které jim dají sami rodiče. Snadno se poté stane, že děti ovládají sociální sítě daleko lépe než například svoji hygienu. Například Facebook je pro ně už naprostou povinností. Kdo ho nemá, nemá v kolektivu šanci na úspěch.[4] Dnešní moderní doba nám mnohdy ani nedává jinou možnost, než s internetem a potažmo sociálními sítěmi pracovat. Tyto skutečnosti opět nahrávají pachatelům.

Kyberkriminalita začala být v České republice tématem už v 90. letech 20. století. V té době se internet začal stávat běžnou součástí našich životů. První případy internetových podvodů byly relativně jednoduché, šlo v nich zejména o podvodné vylákání citlivých údajů oběti. Postupem času se však metody podvodníků staly sofistikovanějšími. Pachatelé se v rámci této trestné činnosti dokážou vždy poučit ze svých chyb a nezdarů. Následně tedy poté přichází s dalším, více promyšleným a do detailů propracovaným plánem, jak dosáhnout svého cíle. V dnešní době jde pachatelům zejména o naše citlivé údaje, jako jsou naše osobní údaje nebo přihlašovací údaje do aplikací, které používáme a o naše peníze. Velkou výhodou pro pachatele a zároveň velkou komplikací pro policii je to, že pachatelé dokážou v dnešní době téměř dokonale skrýt svou totožnost a také místo, odkud na své oběti útočí.

Policie České republiky začala sledovat počet trestných činů spáchaných v kyberprostoru v roce 2011. Počet případů od té doby každoročně narůstá. Největší zlom však přišel v době pandemie onemocnění Covid19, kdy jsme byli nuceni pracovat, učit se a komunikovat právě zejména pomocí internetu a sociálních sítí.

Do tohoto prostoru se tak dostali uživatelé, kteří do té doby s internetem neměli tolik zkušeností, neboť ho do té doby k práci buďto vůbec nepotřebovali nebo jej využívali minimálně. Sociální sítě jsou pro většinu z nás jistou formou zábavy a uvolnění. Navazujeme pomoci nich mezilidské kontakty, učíme se, pomáhají nám překonávat sociální izolaci a pro spoustu z nás jsou také zdrojem příjmů. Toho všeho můžeme dosáhnout i z pohodlí našeho domova, a není k tomu potřeba vyvíjet nijak zvlášť velké úsilí. Ve svém domově se zpravidla cítíme bezpečně. Jenomže nebezpečnost sociálních sítí se jejich domácím užíváním nikterak nesnižuje. Na tento fakt spousta lidí zapomíná. Na sociálních sítích se v teple domova cítí bezpečně a už mnohdy nejsou tak ostražití, jak by měli. To samozřejmě dává šanci pachatelům internetových podvodů. Z neopatrnosti

[4] ŠALMON, T. *(Ne)bezpečný internet, Sprievodca pre používateľov internetu od 10 do 99 rokov*. Bratislava: Lindeni, 2021. s. 18.

uživatelů poté pramení úspěchy podvodníků. Ty mají zase za následek velké počty oznámení, se kterými se posléze musí popasovat policie.

Role Policie České republiky je v boji proti internetovým podvodům naprosto klíčová. Policie nejenže vyšetřuje a stíhá pachatele této trestné činnosti, ale také hraje významnou roli v informování a vzdělávání veřejnosti. Jednou z největších zbraní Policie České republiky v boji proti zejména internetovým podvodům, je prevence. Policie ji realizuje prostřednictvím nejrůznějších kampaní a preventivních programů. Snaží se tím zvýšit povědomí o rizicích spojených s kyberkriminalitou a poskytovat rady, jak se před těmito hrozbami chránit.

Důležitá je také spolupráce policie s médii. Ne každý má vždy možnost, zúčastnit se přednášky či školení. V informování veřejnosti hrají důležitou roli nejen policejní preventisté, ale i tiskoví mluvčí policie. Jejich prací je v tomto ohledu informovat veřejnost o hrozbách spojených s internetovými podvody zejména pomocí tiskových zpráv. S tiskovými zprávami je to dalo by se říct stejné, jako s články novinářů. Čím zajímavější tisková zpráva je, tím vetší vzbudí zájem. Informace, která je formou tiskové zprávy veřejnosti sdělována, se poté může snáze dostat například i do rádií, případně až do hlavních zpráv některé z předních českých televizí. Informaci se tak může dozvědět daleko více lidí nejrůznějších věkových skupin. A o to především jde. Aby se například o nové metodě podvodníků dozvědělo v co nejkratším čase co nejvíce lidí.

I proto bylo jedním z cílů mé bakalářské práce zjistit, jak je Policie České republiky efektivní v informování veřejnosti o metodách internetových podvodníků.

1 Cíl a metodika bakalářské práce

Hlavním cílem bakalářské práce bylo posoudit typy internetových podvodů a jejich četnost na území České republiky s důrazem na aktuální hrozby. Prvním vedlejším cílem bylo zhodnotit efektivitu a metody informování veřejnosti o internetových podvodech ze strany Policie České republiky, včetně preventivních kampaní a dostupnosti informačních zdrojů. Druhým vedlejším cílem bylo navrhnout doporučení ke zlepšení informovanosti veřejnosti s cílem zvýšit povědomí o rizicích a prevenci internetových podvodů.

Bakalářská práce je rozdělena na část teoretickou a empirickou. K vypracování teoretické části bakalářské práce bylo využito studium odborné literatury a dalších odborných zdrojů. Praktická část bakalářské práce byla zpracována formou výzkumného šetření, které bylo koncipováno kvalitativně, za použití metody dotazování, technikou řízených rozhovorů u osob z každé věkové skupiny – nezletilý, mladistvý, dospělý, senior. Bylo zjišťováno, zda je informovanost veřejnosti ohledně internetových podvodů ze strany Policie České republiky dostatečná.

Bakalářská práce je rozdělena do sedmi kapitol spolu s úvodem a závěrem, dále je rozšířena o výzkumné šetření, které se zabývalo mírou informovanosti veřejnosti ohledně internetových podvodů.

V první kapitole je uveden cíl bakalářské práce, použité metody a zdroje, které byly využity při studování a psaní této práce.

Druhá kapitola se zabývá obecným výkladem kybernetické trestné činnosti, základními pojmy, její historií a vývojem.

Ve třetí kapitole jsou představeny jednotlivé metody pachatelů kybernetické trestné činnosti. Rozebírám zde nejčastější způsoby podvodného jednání. Zaměřuji se zde také na pachatele a oběti této trestné činnosti.

Ve čtvrté kapitole analyzuji konkrétní způsob podvodného jednání. Zabývám se tím, kde pachatelé tohoto policií nejčastěji evidovaného podvodu působí a jakým způsobem podvod probíhá. Rozebírám dopad na oběti, cílovou skupinu pachatelů a v neposlední řadě zmiňuji opatření bank a opatření Policie České republiky.

Pátá kapitola se věnuje zákonům a předpisům, které se týkají internetových podvodů v České republice.

Šestá kapitola se zabývá bojem Policie České republiky proti internetovým podvodům. Představuji zde specializované útvary, které se zaměřují na boj proti internetový podvodům a rozebírám jejich vyšetřování. Dále se zde věnuji preventivní činnosti Policie České republiky.

Sedmá kapitola je praktickou částí bakalářské práce, která se zabývá vedlejšími cíli. Je zde primárně posouzena otázka, zda je informovanost veřejnosti ohledně internetových podvodů ze strany Policie České republiky dostatečná.

Poslední, osmá kapitola shrnuje celou teoretickou část bakalářské práce, věnující se internetovým podvodům, i praktickou část bakalářské práce, která se zabývala výzkumným šetřením. V diskusi rovněž poukazuji na možné zlepšení strategie informovanosti veřejnosti ohledně internetových podvodů ze strany Policie České republiky.

2 Obecný výklad kybernetické trestné činnosti

V dnešní době prakticky neexistuje lidská činnost, která by přímo nebo nepřímo nevyužívala počítače ve spojení s dalšími zařízeními, jako jsou tiskárny či skenery. Všechna tato zařízení jsou označována jako výpočetní technika. Tato technika je ve velké míře propojována do vnitřních firemních sítí, ale také samozřejmě k internetu, tedy do kyberprostoru. Dnešní moderní doba umožnila, že funkci počítače dnes přebírají i jiná zařízení, jako jsou mobilní telefony nebo tablety, které se staly součástí výpočetní techniky. Proto nelze pojem počítačová kriminalita chápat pouze jako trestné činy spáchané pomocí počítače připojeného k internetu. Pachatelé dnes k páchání trestné činnosti využívají i telefony a tablety, které jsou často připojeny k internetu. Bez tohoto připojení by tato zařízení byla prakticky nepoužitelná a neplnila by svůj účel. Tím se tak i tato zařízení stala objektem počítačové kriminality.[5]

Co je vlastně kyberprostor? Jedná se o virtuální prostředí, které uživatelům po celém světě umožňuje online komunikaci, sdílení informací, fotek, videí a v neposlední řadě se vzájemně ovlivňovat a poznávat se. Zahrnuje prakticky veškeré aktivity, které můžeme dělat pomocí internetu, jako jsou e-maily, sociální sítě, online obchody a další již v dnešní době běžné služby. Kyberprostor se velice často dynamicky mění. Mění se technologie, nabízené služby i chování jeho uživatelů. Technologie jsou stále složitější, změny přicházejí rychle a často, což způsobuje, že běžný uživatel si neuvědomuje, kolik informací o sobě odhaluje v kyberprostoru. Snadno tak může přijít o svá data nebo se stát obětí kybernetické kriminality.[6]

Moderní technologie současné doby zajistili to, že na nás pachatelé kybernetické trestné činnosti mohou útočit prakticky odkudkoliv a především kdykoliv. Již nemusí využívat počítač či notebook, který je připojený k internetu. Internet je dnes pomocí wifi dostupný téměř všude, včetně prostředků městské či dálkové dopravy. Pro většinu světa se internet stal prakticky běžnou věcí, bez které si v dnešní době už spoustu záležitostí ani nevyřídíme. Dnešní doba nás prakticky nutí k tomu, pořizovat si chytré mobilní telefony a pracovat s internetem. Ohledy se v tomto řekněme technologickém pokroku

[5] KOLOUCH, J., BAŠTA, P., KROPÁČKOVÁ, A. a KUNC, M. *CyberSecurity*. Praha: CZ.NIC, 2019. s. 16-19.
[6] KOHOUT, R., KLOZOVÁ, M. *Internetem bezpečně (nejen) pro seniory*. Karlovy Vary: you connected, 2020. s. 10.

neberou téměř na nikoho. Do kyberprostoru se dostávají osoby, které v něm neumí nebo vůbec nechtějí pracovat. To z nich dělá pro pachatele kybernetické kriminality snadnou kořist.

2.1 Základní pojmy

Pojmů, které se týkají problematiky kybernetické trestné činnosti je velké množství. Níže vysvětlím ty nejzákladnější a také ty, které zároveň obsahuje tato práce.

Kybernetická trestná činnost – Dříve nazývaná též jako informační kriminalita, je definována jako trestná činnost, páchaná v prostředí informačních a komunikačních technologií včetně počítačových sítí.[7]

Kyberprostor – Prostředí, které je tvořené počítačovými sítěmi a jednotlivými prvky těchto sítí, jako jsou například jakákoliv zařízení, mající přidělenou IP adresu, tedy počítače, ale i cokoliv jiného, co umí komunikovat s jinými zařízeními.[8]

Internet – Jedná se o globální síť, která propojuje menší sítě, jako jsou ty v práci, ve školách nebo doma. Tvoří jej všechna zařízení, která jsou schopná komunikace přes internet, například počítače, tablety, telefony nebo televizory.[9]

Hacking – Jedná se o činnost, jejímž cílem je překonání zabezpečení počítačového systému a získání přístupu k datům oběti, s nimiž pak může pachatel nakládat podle svého uvážení.[10]

Internetové podvody – Do detailu promyšlené protiprávní jednání pachatele.[11] Cílem je vylákat z obětí finanční prostředky, případně citlivé informace. Citlivými informacemi se v tomto případě rozumí osobní údaje či údaje o internetovém bankovnictví a platebních kartách.

[7] Policie České republiky. *Kyberkriminalita* [online]. [cit. 11.02.2025]. Dostupné z: https://policie.gov.cz/clanek/kyberkriminalita.aspx
[8] SMEJKAL, V. *Kybernetická kriminalita*, *3. vydání*. Plzeň: Aleš Čeněk, 2022. s. 21.
[9] KOHOUT, R., KLOZOVÁ, M. *Internetem bezpečně (nejen) pro seniory*. Karlovy Vary: you connected, 2020. s. 10.
[10] Policie České republiky. *Jednotlivé druhy kyberkriminality* [online]. [cit. 13.02.2025]. Dostupné z: https://policie.gov.cz/clanek/jednotlive-druhy-kyberkriminality.aspx
[11] Policie České republiky. *Pomoc obětem TČ, Počítačová kriminalita* [online]. [cit. 13.02.2025]. Dostupné z: https://policie.gov.cz/clanek/pomoc-obetem-tc-pocitacova-kriminalita.aspx

Phishing – Pachatel se pomocí emailu s odkazem snaží nasměrovat oběť na podvodnou stránku, pomocí které se následně pokouší získat citlivé informace oběti. Ty následně zneužije nebo poté případně zpeněží.[12]

Vishing – Podvodná metoda, která pro účely útoku nevyužívá webové stránky. Pachatelé útočí prostřednictvím zpráv, které nabádají potenciální oběti, aby se ozvaly na konkrétní telefonní číslo a následně při telefonátu sdělili své citlivé údaje.[13]

Smishing – Lákání citlivých údajů obětí pomocí SMS zpráv. Citlivými údaji se zde rozumí rodná čísla nebo přístupová hesla k bankovním službám.[14]

Reverzní inzerát – Jednání v rámci, kterého pachatel zareaguje na podaný inzerát a při následné komunikaci pod legendou zájmu oběti podstrčí podvodnou platební bránu. Po vyplnění citlivých údajů následně oběť přichází o peníze.[15]

Nigerijské dopisy – Způsob podvodného jednání, při kterém pachatelé sázejí zejména na kvantitu. Mezi oslovenými se vždy najde někdo, kdo bude slyšet na cenný balíček, pomoc v nouzi či se nechá zmanipulovat falešným dojmem, že jej pachatel miluje.[16]

Dark Web – Záměrně skryté webové stránky, na které lze vstoupit jen pomocí speciálního softwaru. Běžný uživatel internetu se na jeho stránky nedostane. Probíhají zde obchody s legálním, ale zejména s nelegálním zbožím (drogy, zbraně, padělky peněz a dokladů, odcizené údaje o kreditních kartách a přístupové údaje k účtům všech druhů a jiné).[17]

2.2 Historie a vývoj kybernetické trestné činnosti

Na vznik počítačové kriminality mají vliv dva klíčové faktory. Prvním je samotné vytvoření počítače. První počítače byly obrovské a zabíraly celé místnosti. Díky technologickému pokroku se počítače zmenšily a jejich výkon se zlepšil. Významný

[12] ŠULC, V. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018. s. 68.
[13] KOŽÍŠEK, M. a PÍSECKÝ, V. *Bezpečně n@ internetu: průvodce chováním ve světě online.* Praha: Grada Publishing, 2016. s. 126.
[14] Policie České republiky. *Preventivní informace, Smishing* [online]. [cit. 14.02.2025]. Dostupné z: https://policie.gov.cz/clanek/preventivni-informace-smishing.aspx
[15] Policie České republiky. *nePINdej* [online]. [cit. 14.02.2025]. Dostupné online z: https://policie.gov.cz/clanek/nepindej.aspx
[16] Tamtéž.
[17] SMEJKAL, V. *Kybernetická kriminalita*, *3. vydání*. Plzeň: Aleš Čeněk, 2022. s. 94.

posun nastal v 80. letech 20. století, kdy byl vyroben první osobní počítač IBM, který byl cenově dostupný pro širokou veřejnost. To umožnilo, aby se počítače dostaly do domácností a vznikl tak osobní počítač.[18]

Druhým klíčovým faktorem pro vznik počítačové kriminality byla už v té době existující telefonní síť, která byla běžně používána ve společnosti. V 70. letech 20. století byl k této síti přidán systém Bulletin Board System, který umožnil propojení osobních počítačů s telefonní sítí. Tento systém předcházel masovému rozšíření internetu, jak ho známe dnes. Lidé se k Bulletin Board Systému připojovali pomocí modemu a vytáčením telefonní linky. Díky zmíněnému systému začali uživatelé sdílet různé informace, čímž vznikla první forma kyberprostoru.[19]

V 80. letech 20. století vznikla v USA hackerská skupina, která se svými útoky zaměřovala převážně na telefonní síť. V průběhu 80. a 90. let 20. století byly v USA provedeny první hackerské útoky na telekomunikační společnosti a banky.[20]

V roce 1968 byly poprvé propojeny počítače do sítě zvané Arpanet, což zahrnovalo čtyři univerzitní počítače sdílející informace. Tento krok položil základy pro vznik internetu. V 90. letech 20. století byla spuštěna samotná síť Internet, představily se první webové stránky a vznikl WWW server. Od roku 1993 se internet začal masově rozšiřovat, což vedlo k rozvoji nových informačních technologií a vzniku kyberprostoru, jak ho známe dnes. Tento rozmach také přispěl k nárůstu počítačové kriminality, což se v 90. letech 20. století stalo běžným termínem pro trestnou činnost páchanou pomocí počítačů v prostředí internetu, tedy kyberprostoru.[21]

V současné době však v páchání kybernetické trestné činnosti hrají velkou, ne-li zásadní roli mobilní telefony. Stejně jako počítače se i mobilní telefony postupem času zdokonalovaly. Dnešní realita se s prvními mobilními telefony nedá vůbec srovnávat. Dnes již prakticky nekoupíme nový mobilní telefon, který by dokázal plně fungovat bez podpory internetu. Stále dokážeme bez internetu z telefonu někomu zavolat nebo mu poslat textovou zprávu, nemohli bychom ale bez něho využít většinu pro nás již běžných funkcí, které dnešní mobilní telefony nabízejí. Většina lidí dnes používá internet

[18] KOLOUCH, J. *Cyberkrime.* Praha: CZ.NIC, 2016. s. 11-16.
[19] BEDNÁŘ, V. *Internetová publicistika*, *Žurnalistika a komunikace*. Praha: Grada Publishing, 2011. s. 34-43.
[20] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, 2016. s. 11-16.
[21] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada Publishing, 2007. s. 15-16.

především prostřednictvím mobilních zařízení, jako jsou chytré telefony nebo tablety. Bohužel, mnoho z těchto zařízení není dostatečně zabezpečeno. Ne všichni výrobci mobilních telefonů totiž věnují dostatečnou pozornost bezpečnosti uživatelů tak, jak by měli.[22]

Většina Evropanů nosí v dnešní době u sebe běžně jedno nebo více mobilních zařízení. Mobilní aplikace dnes pokrývají víceméně všechny oblasti života. Mnoho lidí také používá svá zařízení jak pro osobní, tak pracovní účely. Zneužívání těchto zařízení různými formami kyberkriminality proto rychle roste.[23]

Pachatelé mají různé důvody k používání mobilních telefonů pro své aktivity. Z mého hlediska jsou to především anonymita a možnost přinejmenším znesnadnit své vypátrání. Pomocí například předplacené SIM karty nebo nejrůznějších aplikací dokážou pachatelé téměř dokonale skrýt svou totožnost. Mobilní telefon se dá také různými způsoby šifrovat, což znesnadňuje jeho sledování. Dalším důvodem může být mobilita. Mobilní telefony jsou totiž snadno přenosné a dají se lehce ukrýt nebo někam propašovat. Mobilní telefony samozřejmě umožňují také snadnou a rychlou komunikaci. Nelze přehlédnout ani rostoucí úroveň a kreativitu škodlivých programů, které pachatelé používají k útokům na systémy a aplikace pro Android, iPhone a další platformy.[24] V neposlední řadě jsou to informace, které lze na mobilním telefonu pomocí internetu vyhledat.

2.3 Statistiky kybernetické trestné činnosti

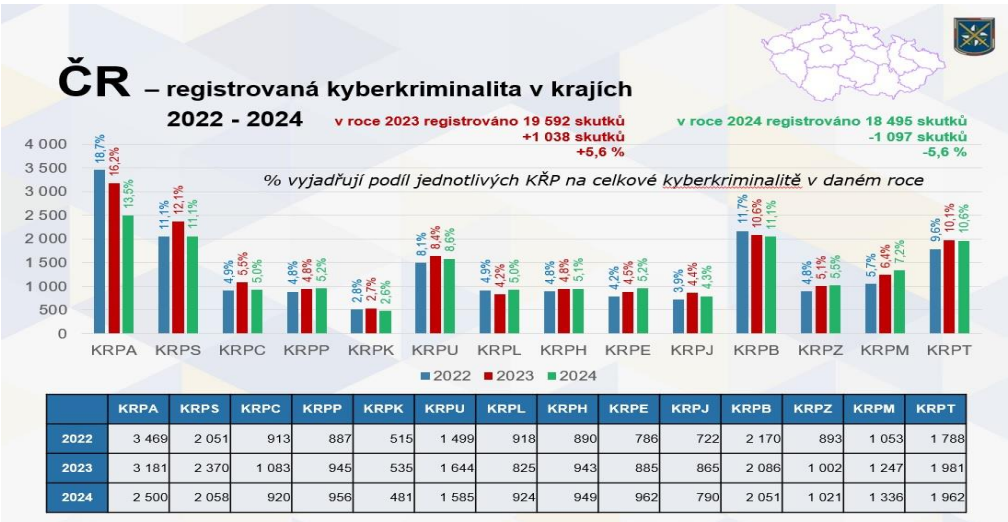
Než se budu zabývat statistikou kybernetické trestné činnosti, pojďme si nejprve ukázat statistiku podílů jednotlivých druhů trestné činnosti na celkovou kriminalitu v České republice za uplynulý rok 2024. Podotýkám, že statistiku kybernetické trestné činnosti zde nenajdeme, neboť ta se statisticky sleduje zvlášť.

[22] KOHOUT, R., KLOZOVÁ, M. *Internetem bezpečně (nejen) pro seniory*. Karlovy Vary: you connected, 2020. s. 13.
[23] ŠULC, V. a kolektiv autorů. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech*. Praha: Policejní akademie České republiky, 2020. s. 28
[24] Tamtéž, s. 20.

Obr. 1: Podíl druhů trestné činnosti na celkové kriminalitě, Česká republika, období 1. 1.-31. 12. 2024. [statistika]. Základní statistické údaje o kriminalitě, leden-prosinec 2024 v meziročním srovnání. Praha: 2025, str. 5.

V uplynulém roce 2024, tvořila kybernetická trestná činnost přes 10% celkové kriminality, kterou Policie České republiky registrovala. Celkem bylo evidováno 18 495 trestných činů, spáchaných v kyberprostoru.[25] Následující statistika ukazuje, jakými čísli se podílelo všech čtrnáct krajských ředitelství policie. Statistika ukazuje také počet evidované kybernetické trestné činnosti v jednotlivých krajích za roky 2022 a 2023.

Obr. 2: ČR-registrovaná kyberkriminalita v krajích, 2022-2024. [statistika]. Základní statistické údaje o kriminalitě, leden-prosinec 2024 v meziročním srovnání. Praha: 2025, str. 13.



	KRPA	KRPS	KRPC	KRPP	KRPK	KRPU	KRPL	KRPH	KRPE	KRPJ	KRPB	KRPZ	KRPM	KRPT
2022	3 469	2 051	913	887	515	1 499	918	890	786	722	2 170	893	1 053	1 788
2023	3 181	2 370	1 083	945	535	1 644	825	943	885	865	2 086	1 002	1 247	1 981
2024	2 500	2 058	920	956	481	1 585	924	949	962	790	2 051	1 021	1 336	1 962

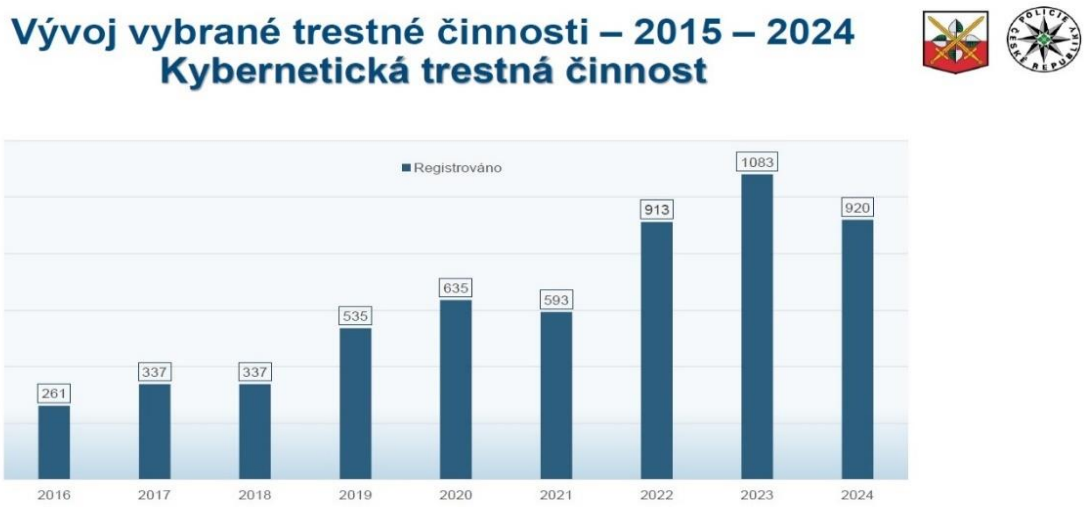
[25] Policie České republiky. *Vývoj registrované kriminality v roce 2024* [online]. [cit. 14.02.2025]. Dostupné z: https://policie.gov.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2024.aspx

Je nutné poznamenat, že statistika pracuje pouze s oznámenými trestnými činy. Reálná čísla mohou být daleko vyšší. Stejně tak je nutné zdůraznit, že v případě trestných činů, kde má zásadní vliv na právní kvalifikaci způsobená škoda, se do statistik nezapočítávají oznámené případy, při nichž poškozenému nevznikla škoda nikoliv nepatrná, tedy škoda vyšší, než 10 000 korun.

V případě kybernetické trestné činnosti, je důležité vědět, že se do této statistiky započítávají všechny trestné činy, které byly spáchány prostřednictvím internetu nebo jiných informačních technologií.

Internetové podvody se staticky řadí do kybernetické trestné činnosti, proto se samostatně statisticky nesledují. Pro zajímavost níže ještě uvádím statistiku kybernetické trestné činnost, kterou evidovala jihočeská policie v letech 2015 až 2024. Na tuto statistiku se podíváme trochu blíže.

Obr. 3: Vývoj vybrané trestné činnosti-kybernetické kriminality v letech 2015-2024. [statistika]. Prezentace výsledků za rok 2024. Vývoj vybrané trestné činnosti-2015-2024, Kybernetická trestná činnost. České Budějovice: 2024, str. 32.



Z uvedené statistiky můžeme vyčíst, že největší nárust kybernetické trestné činnosti zaznamenala jihočeská policie v letech, kdy jsme čelili celosvětové pandemii onemocnění Covid19. Nejvíce skutků evidovali policisté z jihočeského kraje v roce 2023. V roce 2024 však nastal mírný pokles. Jedním z důvodů může být i snaha ze strany Oddělení tisku a prevence, o němž bude v této práci také řeč. Případů je však stále velké množství. Jak jsem ale již také zmínil, reálná čísla budou pravděpodobně daleko vyšší.

3 Internetové podvody současné doby

Internetové podvody jsou druhem kybernetické trestné činnosti, který v současné době zaměstnává Policii České republiky úplně nejvíce. V dnešním moderním světě se internet stal nedílnou součástí našeho každodenního života. S rostoucím počtem uživatelů a rozšiřujícími se možnostmi online služeb přichází ale i zvýšené riziko internetových podvodů. Tyto podvody představují v současné době velkou hrozbu. Ohroženi jsme prakticky všichni, a to bez ohledu na věk či stupeň dosaženého vzdělání. V této kapitole se zaměřím na různé typy internetových podvodů, jejich charakteristiky a způsoby, jak se před nimi chránit.

3.1 Definice internetových podvodů

Podle trestního zákoníku se dopustí trestného činu podvodu ten, kdo se obohatí tím, že někoho uvede v omyl, využije jeho omylu nebo zamlčí důležité skutečnosti, a tím způsobí škodu na cizím majetku.[26] V případě trestných činů se musí jednat o škodu nikoli nepatrnou, tedy škodu vyšší než 10 000 korun.

S rozvojem internetu a online služeb se výrazně zvýšil počet internetových podvodů. Díky nepřímému kontaktu s oběťmi, téměř neomezenému počtu potenciálních cílů a nízkému riziku odhalení se stal internet doslova rájem pro pachatele této trestné činnosti.[27] Níže uvádím nejčastěji využívané způsoby podvodného jednání.

3.2 Sociální inženýrství

Existuje mnoho způsobů, jak mohou lidé na internetu podvádět, okrádat nebo zneužívat jeho ostatní uživatele. Internet sám o sobě je bezpečný, ale nebezpečí představují lidé, kteří na něm působí. Tito lidé, zejména pachatelé trestné činnosti, neustále hledají nové způsoby, jak dosáhnout svých cílů. Ve skutečném životě může stačit vytrhnout někomu peněženku z ruky. Na internetu je ta peněženka, ale vzdálená a útočníci

[26] KOŽÍŠEK, M. a PÍSECKÝ, V. *Bezpečně n@ internetu: průvodce chováním ve světě online.* Praha: Grada Publishing, 2016. str. 111.
[27] Tamtéž.

se k ní musí dostat, různými, rafinovanými metodami. Tyto metody jsou často velmi propracované a pachatelé je neustále mění a zdokonalují, aby byly co nejúspěšnější.[28]

Mnozí lidé žijí v přesvědčení, že k ochraně na internetu postačí dlouhé heslo, nainstalovaný antivir a bezpečné připojení z domova. Sociální inženýři nevyužívají hrubou sílu k dosažení svého cíle, jejich útok je sofistikovaný a má několik fází. Neplýtvají úsilím a nesnaží se prolomit heslo přes útok, protože vědí, že daleko jednodušší je zeptat se na něj přímo oběti.[29]

3.2.1 Phishing

Phishing je dalo by se říct dokonalým příkladem sociálního inženýrství, což je metoda manipulace lidí za účelem provedení útoku nebo získání specifických informací. Útočníci často nejsou v přímém kontaktu s obětí. Útoky zahrnují prvky přesvědčování a manipulace a mohou být prováděny náhodně nebo cíleně na konkrétní osoby. Útočníci se často učí z chyb, které během útoků udělali, a neustále své metody zdokonalují a přizpůsobují.[30]

Dá se tedy říct, že za phishing lze označit jakoukoliv činnost pachatele, která bezprostředně směřuje k získání citlivých informací od oběti. Pachatelé se většinou snaží získat především přihlašovací údaje do internetového bankovnictví, případně získat potřebné údaje z naší platební karty. Stěžejními údaji jsou v tomto případě číslo platební karty, její platnost a zadní třímístný bezpečnostní kód. Pokud pachatel tyto tři údaje získá, může naší platební kartu odcizit, aniž by nám musel sahat do peněženky. Pachatelé se tyto informace snaží získávat nejrůznějšími způsoby. Hojně využívané jsou falešné e-maily.

Phishing už ale dávno není jen o e-mailech, i když ty jsou stále oblíbeným způsobem útoku. Čím dál častěji se setkáváme se zneužitím SMS zpráv, sociálních sítí,

[28] KOŽÍŠEK, M. a PÍSECKÝ, V. *Bezpečně n@ internetu: průvodce chováním ve světě online.* Praha: Grada Publishing, 2016. str. 36.
[29] Tamtéž.
[30] KOŽÍŠEK, M. a PÍSECKÝ, V. *Bezpečně n@ internetu: průvodce chováním ve světě online.* Praha: Grada Publishing, 2016. str. 37.

falešných webových stránek, a dokonce i telefonních hovorů, kde se útočníci nejčastěji vydávají za pracovníky bank, úřadů nebo poskytovatele služeb.[31]

3.2.2 Vishing

Tento druh podvodu principiálně spočívá v telefonních hovorech, při kterých se pachatel obvykle vydává za pracovníka některé z bank, který údajně zjistil napadení bankovního účtu, čímž se tak snaží vystrašit osobu, které volá. Tvrdí, že je nutné okamžitě převést finanční prostředky na jiný účet, s příslibem, že budou po vyřešení situace vráceny, což se však nestane. Jeho hlavním cílem je získat finanční prostředky oběti, případně přihlašovací údaje do internetového bankovnictví. Tento typ podvodu je obzvláště nebezpečný, protože falešní bankovní pracovníci mohou již před hovorem znát různé informace o osobách, které kontaktují.[32]

Volání podvodných bankéřů či investičních poradců je druhem internetových podvodů, se kterým se Policie České republiky setkává prakticky denně. Mezi poškozenými jsou osoby všech věkových kategorií a všech stupňů dosaženého vzdělání. Škody jdou mnohdy do milionů korun. Je však nutno konstatovat, že jakmile oběť pachateli uvěří a peníze buďto pošle nebo mu zpřístupní své internetové bankovnictví, tak odcizené peníze velice pravděpodobně už nikdy neuvidí. Objasněnost těchto případů se pohybuje v nižších jednotkách procent. U phishingu jsem uvedl, že se pachatelé učí ze svých chyb a nezdarů. V případě těchto podvodů pachatelé například místo běžné platby využívají platbu tak zvaně okamžitou. Jakmile odešleme peníze pomocí okamžité platby, jsou peníze z našeho účtu pryč do pár vteřin. Vůbec přitom nezáleží, kdy a kam peníze posíláme. Odcizené peníze jdou také většinou okamžitě na zahraniční účty. Nejlépe do zemí, se kterými nemá Česká republika uzavřenou dohodu o spolupráci, natož o policejní spolupráci. Policisté jsou po několikaměsíční práci schopni dohledat, kam, případně do jaké banky peníze odešly, nicméně nemají zákonnou oporu v tom, odcizené finanční prostředky zajistit a vrátit poškozené osobě.

[31] ŠULC, V. a kolektiv autorů. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech*. Praha: Policejní akademie České republiky, 2020. str. 28.
[32] Policie České republiky. *Současné trendy podvodníků – vishing a spoofing* [online]. [cit. 09.01.2025]. Dostupné z: https://policie.gov.cz/clanek/prevence-rady-a-doporuceni-soucasne-trendy-podvodniku-vishing-a-spoofing.aspx

3.2.3 Smishing

Jedná se o způsob podvodu, který je realizovaný pomocí textových zpráv. Pachatel se v těchto případech většinou snaží telefonní číslo, ze kterého zprávu odesílá, vydávat za telefonní číslo banky, úřadu nebo doručovací společnosti. Tyto často nevyžádané textové zprávy obsahují ve většině případů různé odkazy, které vybízejí k vyplnění osobních údajů, potvrzení přístupových hesel nebo k povolení vzdáleného přístupu do mobilního telefonu adresáta.[33]

Nezáleží na tom, zda pachatel použije phishing, vishing nebo smishing, jeho motivací bude vždy jen to, okrást svou oběť o co největší finanční obnos. Postupem času pachatelé svá podvodná jednání neustále zdokonalují a snaží se být vždy ten jeden pomyslný krok před policií. V tomto ohledu je pro ně velkou pomocí i dnešní moderní technika a aplikace.

3.3 Spoofing

V této kapitole byly popsány nejzákladnější druhy kybernetické trestné činnosti. Dále je potřeba vysvětlit, jak je možné, že jsou pachatelé tak úspěšní, jaká technika jim ten úspěch přináší. Jedná se o techniku zvanou spoofing. Ta spočívá v tom, že pachatel prakticky napodobí telefonní číslo, e-mail či webovou stránku a následně se za ně vydává. Spoofing pachatelé využívají nejčastěji u podvodů, v rámci kterých se vydávají za pracovníky bank nebo investičních společností.

3.3.1 Spoofing webových stránek

Jedná se o velmi nebezpečný a ze strany pachatelů hojně využívaný způsob podvodu. V dnešní době se totiž najde jen velmi málo lidí, kteří mají účet u některé z bank, ale nemají zároveň zřízené internetové bankovnictví. Stejně internetové nákupy či prodej zboží jsou již v dnešní době naprosto běžnou věcí. Tohle všechno pachatelé samozřejmě vědí, proto ke spoofingu kupříkladu nejrůznějších e-shopů či webových stránek bank přistupují. Spoofing webové stránky nemusí mnohdy odhalit ani pokročilý

[33] Policie České republiky. *Smishing* [online]. [cit. 09.01.2025]. Dostupné z: https://policie.gov.cz/clanek/smishing.aspx

uživatel internetu. Stránka je totiž mnohdy naprosto k nerozeznání od té skutečné. Rozdíl se většinou skrývá pouze v názvu domény. V názvu podvodné webové stránky bude oproti té skutečné vždy něco navíc. Často se jedná o jeden znak (písmeno, číslici). Název webové stránky je totiž to jediné, co pachatelé nedokážou dokonale napodobit.

3.3.2 Spoofing telefonního čísla a e-mailu

Princip spoofingu telefonního čísla spočívá v tom, že pachatel sice stále volá ze svého skutečného telefonního čísla, dokáže ho ale skrýt za buďto existující či dokonce i neexitující telefonní číslo. Nejčastěji je využíván při podvodném jednání, v rámci, kterého se pachatelé vydávají za bankéře, případně za policisty.

A právě spoofing telefonních čísel Policie České republiky byl skutečně nepříjemným problémem. Tento trik podvodníků totiž způsoboval, že se skutečná čísla policie stávala pro občany nedůvěryhodnými. Používám minulý čas, neboť se podařilo zajistit, že čísla Policie České republiky tímto způsobem již nelze zneužít. Pochopitelně je zde řeč o mobilních telefonních číslech policie. Tísňovou linku spoofovat nelze.

Ve spoofovaných e-mailech se většinou nachází různé odkazy. Pokud na ně oslovená osoba klikne, odkaz ji přesměruje ve většině případů na podvodnou stránku společnosti, za níž se pachatel vydává.

Záměrem spoofovaných e-mailů není pouze obtěžovat příjemce a zaplnit mu e-mailovou schránku. Snaží se získat přístup k jeho osobním údajům, například k údajům o internetovém bankovnictví nebo k údajům z platební karty, a to právě tím, že ho přesměrují na falešné webové stránky.[34]

Spoofing ať už webových stránek, telefonních čísel či e-mailu, mají vždy společný cíl. Ten spočívá v oklamání adresáta za účelem získání citlivých údajů oslovené osoby. Spoofing ale obětem nemusí způsobit nutně jen finanční ztráty. V případech, kdy se pachatelé vydávají za některou z organizací, může tato organizace utrpět značné poškození své pověsti s následnou ztrátou důvěry zákazníků. V krajních případech může z jejich strany dokonce dojít i k podání trestního oznámení. Možné je i uložení pokuty za nedostatečné zabezpečení dat. V neposlední řadě může spoofing způsobit také výpadky

[34] BROOKSHEAR, J. Glenn. *Informatika.* Brno: Computer Press, 2013. str. 184.

služeb a narušení provozu. S ohledem na výše uvedené, může mít úspěšný spoofing zásadně negativní vliv na další fungování společnosti, za níž se pachatel v rámci svého podvodného jednání rozhodl vydávat.

3.4 Konkrétní způsoby podvodného jednání

V této podkapitole nyní představím konkrétní způsoby jednání pachatelů internetových podvodů. S podvody, které níže uvádím, se Policie České republiky potýká prakticky každý den. Z tohoto důvodu považuji za důležité je v této práci zmínit.

3.4.1 Investiční podvody

Většinou jde o možnost investování do kryptoměn či do akcií úspěšných společností. V přesvědčivé reklamě, která se většinou objevuje na sociálních sítích, investice vychvalují i známé osobnosti. Většinou jde o sportovce, politiky či velmi bohaté a úspěšné osoby. Podvod většinou začíná tím, že oběť vyplní formulář, kde uvede osobní údaje. Jedná se převážně o jméno, příjmení, telefonní číslo a email. Formulář se ve většině případů nachází přímo pod reklamou nebo článkem.

Na základě vyplnění formuláře se oběti v krátké době ozve pachatel a vyzve ji k prvotní investici. Většinou jde o investici v řádu několika tisíců korun, která má sloužit pro založení investiční peněženky, případně investičního účtu. Pachatel následně oběti telefonicky sdělí, že jí bude přidělen zkušený investor, který jí s dalšími investicemi pomůže.

Když pachateli oběť uvěří a pošle peníze, zašle ji falešnou stránku, na které uvidí, že má založený účet a již jsou na něm kladné pohyby. Tento trik má oběť přimět k tomu, aby skutečně uvěřila tomu, že již vydělává a byla ochotna investovat více peněz.

Jeho dalším krokem může být také to, že se oběť pokusí přesvědčit k nainstalování a spuštění programu, pomocí kterého dokáže vzdáleně vstoupit do jejího zařízení, a to s příslibem, že za ni bude vše vyřizovat a obchodovat s větším výdělkem. Jednoduše si oběť za kratší dobu vydělá více peněz. Když mu přístup oběť povolí, prakticky mu tím zpřístupnila internetové bankovnictví a pachatel si s jejími penězi může dělat prakticky co chce.

Další velkou nepříjemností u tohoto podvodu je to, že ze strany policie může být oběť považována za pachatele nebo spolupachatele. Aby pachatel zvýšil uvěřitelnost podvodu, může na účet oběti převést peníze, které „investovali“ další poškození. Na jejím účtu se tak mohou objevit odcizené peníze někoho jiného. Tím však může dojít k naplnění skutkové podstaty trestného činu s názvem legalizace výnosů z trestné činnosti z nedbalosti, který nalezneme v trestním zákoníku pod § 217. Tento paragraf hovoří o tom, že pokud někdo, byť neúmyslným jednáním, pomůže zakrýt původ nelegálně získaného majetku, může za to být trestně odpovědný.[35]

Obr. 4: Podvodná reklama skupiny ČEZ. [online]. Dostupné z: https://www.cez.cz/cs/podvodna-reklama#gallery-5.

3.4.2 Podvod při prodeji zboží

Pachatel zareaguje na inzerát oběti a projeví zájem o koupi jakéhokoliv zboží, které se snaží prodat. Komunikace nejčastěji probíhá pomocí aplikace WhatsApp, případně přes email. Prvotní zpráva pachatele vypadá zhruba takto: „Dobrý den! Je Vaše zboží stále k dispozici? Mám zájem!“ nebo „Dobrý den! Mám zájem o Vaše zboží! Pošlu kurýra.“.

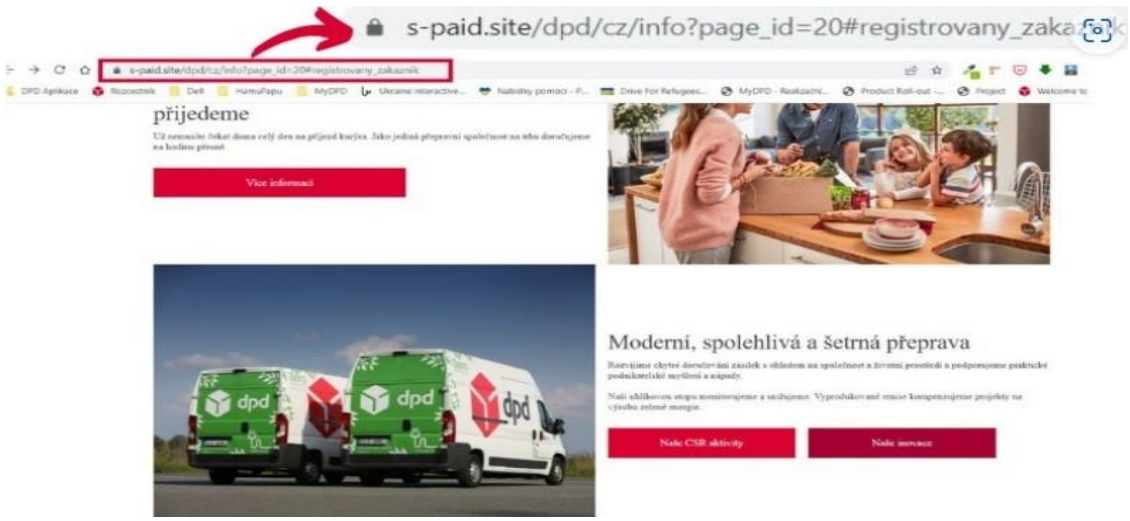
[35] ČESKO. *§ 217 zákona č. 40/2009 Sb., trestní zákoník*. In: Zákony pro lidi.cz [online]. © AION CS 2010–2025 [cit. 21. 2. 2025]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40#p217

Pokud mu oslovený prodávající kladně odpoví, poprosí jej, zda by bylo možné, poslat si pro zboží přepravní společnost, neboť on si nemůže zboží z nejrůznějších důvodů osobně vyzvednout. Také prodávajícího poprosí, zda by nemohl za přepravu zaplatit on, s tím, že mu cenu za přepravu přičte k ceně zboží. Když prodávající souhlasí, vyžádá si od něj pachatel emailovou adresu, na kterou pošle falešný odkaz stránek domluvené přepravní společnosti. Zde má prodávající vyplnit osobní údaje a přihlašovací údaje do internetového bankovnictví.

Dalším způsobem, jak se pachatel v tomto případě bude snažit dostat k penězům oběti je ta, že jí nabídne platbu za zboží na platební kartu. K tomu mu budou stačit pouhé tři údaje. Číslo platební karty, její platnost a zadní třímístný bezpečnostní kód (CVV, CVC, CID). Má to ale háček, platba na platební kartu u nás není možná.

Velké nebezpečí pro nás všechny spočívá v tom, že jediné, co pachatel nedokáže v dnešní době dokonale napodobit, je název domény neboli název internetové stránky, který většinou začíná https://. Vše ostatní bude vždy naprosto k nerozeznání od reality.

Obr. 5: Podvodná stránka přepravní společnosti DPD. [online]. Dostupné z: https://www.dpd.com/cz/cs/bezpecnostni-informace.



3.4.3 Podvody přes seznamky

Pachatelé hledají své oběti obvykle na internetových seznamkách a sociálních sítích. Zde svoji oběť zkontaktují a snaží se ji zlákat a zmanipulovat. Nějakou dobu si s obětí dopisují, posílají své fotografie či videa.

Oběť po nějaké době zjišťuje, že má s pachatelem, nejčastěji s lékařem či vojákem na misi společná témata a zájmy. Jedná se však o dokonalou manipulaci ze strany pachatele. Pachatel slibuje budoucí společný život a zrodí se láska na dálku. Pachatel oběť neustále ujišťuje, že za ni brzy přijede a bude s ní šťastně žít.

Pak přichází zádrhel. Pachatel by rád přijel, ale finanční prostředky na zakoupení letenky nemá na misi k dispozici a chce poslat peníze. Nebo si rovnou řekne o finanční půjčku s legendou pořízení společného bydlení. Slibuje, že všechny peníze vrátí hned, jakmile to bude možné. Další legenda pachatelů spočívá v tom, že oběti sdělí, že se dostali do složité životní situace, ze které jim může pomoci jedině ona.

Dalším způsobem vylákání peněz může být i cenný balíček (šperky, suvenýr), který pachatel oběti údajně posílá. Ta však musí zaplatit související poplatky. Pachatel si tak ověřuje, zda je oslovená osoba ochotna do něho „investovat“. Tuto částku může pak postupně navyšovat až do milionových hodnot.

Podvodníci se většinou zaměřují na ovdovělé, rozvedené či nějakým způsobem doma zanedbávané ženy, u kterých mají logicky největší šanci na úspěch.

3.4.4 Podvody přes mobilní telefon

Mobilní m-platby fungují jako platební karty s rozdílem, že peníze nejsou strženy z bankovního účtu, ale jsou naúčtovány v rámci měsíčního tarifu u mobilního operátora.

Nejčastěji jsou využívány v rámci nákupů her či aplikací přes Obchod play nebo App Store. Zároveň jsou často využívány podvodníky, kteří následně útočí na sociálních sítích. Podvodníci nejčastěji odcizí nebo napodobí něčí profil a následně jeho jménem rozesílají zprávy všem jeho přátelům.

Cílem pachatele je získat jejich telefonní čísla s vymyšlenou legendou o nějaké soutěži. Po získání telefonního čísla žádají ověřovací kód, který přišel oslovené osobě v SMS zprávě. Pod jejím telefonním číslem totiž něco zaplatili. Pokud kód podvodníkovi osoba přepošle, potvrdí platbu.

Zcela záměrně jsem neuvedl nejčastější způsob jednání internetových podvodníků. Je to z důvodu toho, že se mu hlouběji věnuji ve čtvrté kapitole své práce. Na základě shora uvedených příkladů trestné činnosti můžeme vidět, že pachatelé mají

svá jednání opravdu promyšlená. Nechci pachatele samozřejmě nikterak chválit, ale podlehnout jim může opravdu téměř každý.

3.5 Pachatel internetových podvodů

Z pohledu kriminologie můžeme za pachatele označit kteréhokoliv člověka, který spáchal trestný čin. Pachatelé trestných činů se mnohdy mohou vyznačovat sociálně patologickým jednáním. Může se tak jednat například o narkomany, gamblery nebo třeba prostitutky.[36] V případě pachatelů kybernetické trestné činnosti tomu tak ale pravděpodobně nebude.

Druhů kybernetické trestné činnosti je v dnešní době několik. Pokud se však zaměříme čistě jen na internetové podvody, dá se říct, že za útokem velmi pravděpodobně nikdy nestojí jedinec, nýbrž zločinecká organizace. Jedná se o organizované skupiny, zaměřující se na druhy podvodů, jež byly v rámci této kapitoly zmíněny. Lze předpokládat, že pachatelem tohoto druhu trestné činnosti nebude nikdo bez zkušeností v oblasti kybernetiky. A právě například předchozí zkušenosti s páchaním trestné činnosti, případně vzdělání mohou být pro pachatele klíčovými faktory. Nyní se zaměříme na to, co pachatele této trestné činnosti motivuje.

3.5.1 Motiv pachatele

Obecná motivace pachatelů trestných činů může být různorodá a závisí na mnoha faktorech. Mezi nejčastější motivace můžeme zařadit finanční zisk, osobní problémy, pomstu nebo vliv pachatelova okolí. Nyní se blíže podíváme na motivaci pachatelů internetových podvodů.

Ve většině případů jsou hlavními motivy pachatele bezpracný zisk a osobní obohacení.[37] Vedlejšími motivy může být získání prostředků, pomocí kterých se dokážou obohatit bezpracně. V případě internetových podvodů jsou to již několikrát v této práci zmíněné osobní údaje a citlivé údaje, konkrétně přihlašovací údaje k internetovému bankovnictví, případně údaje z platební karty. Další motivací pachatele může být i vědomí toho, že objasněnost této trestné činnosti je velice nízká. Je proto velká

[36] SVATOŠ, R. *Základy kriminologie a prevence kriminality*. České Budějovice: VŠERS, 2009. s 21.
[37] SMEJKAL, V. *Kybernetická kriminalita*, *3. vydání*. Plzeň: Aleš Čeněk, 2022. str. 814.

pravděpodobnost, že při páchání této činnosti bude nejen úspěšný, ale zároveň bude pro policii těžké jej odhalit a dohnat ke spravedlnosti.

3.5.2 Předchozí kriminální zkušenost pachatele

Předchozí kriminální zkušenost pachatele výrazně ovlivňuje jeho metody páchání trestné činnosti. Pachatel se postupně zdokonaluje ve svých technikách a snaží se vyhnout chybám, které udělal v minulosti.[38]

3.5.3 Vzdělání pachatele a jeho pracovní kvalifikace

Vzdělání a pracovní kvalifikace pachatele se nejvíce projevují při páchání trestných činů, které vyžadují specifické znalosti nebo dovednosti. Čím složitější je způsob provedení a jeho jednotlivé části, tím více závisí na těchto faktorech.[39] Z tohoto hlediska lze říct, že páchání kybernetické trestné činnosti, konkrétně internetových podvodů je způsobem páchání jednou z těch složitějších trestných činností. Pachatelé internetových podvodů jsou ve většině případů výmluvní a působí dojmem, že problematice v rámci, které podvody páchají, rozumí. Z těchto důvodů lze usuzovat, že pachatel musí před spácháním podvodu vyvinout určitou snahu a například se vzdělat, případně rozšířit již získané znalosti, které o problematice měl.

3.5.4 Věk pachatele

Věk pachatele ovlivňuje způsob páchání trestné činnosti jak z hlediska jeho psychických, tak fyzických schopností. Tyto faktory souvisí s vývojem a stárnutím lidského organismu. Vyšší věk a s ním spojené životní zkušenosti mohou mít vliv na provedení složitějších trestných činů.[40] U internetových podvodů však nelze s jistotu tvrdit, že pachatelé jsou mladšího či staršího věku. S rostoucím rozšířením počítačů, počítačových sítí a připojení k internetu dochází i v této oblasti k posunu. Věkové

[38] STRAUS, J., PORADA, V. a kolektiv. *Teorie, metody a metodologie kriminalistiky*. Plzeň: Aleš Čeněk, 2017. str. 64.
[39] Tamtéž.
[40] STRAUS, J., PORADA, V. a kolektiv. *Teorie, metody a metodologie kriminalistiky*. Plzeň: Aleš Čeněk, 2017. str. 63-64.

rozložení pachatelů se stává rovnoměrnějším. Věkové rozmezí pachatelů se pohybuje v rozmezí od 17 do 58 let. V průměru je tedy pachatelům 34 let. Bezmála polovině pachatelům je však méně než 30 let.[41] Mladší ročníky sice nemají takové životní zkušenosti, nicméně na rozdíl od starších vyrůstaly a vyrůstají v době internetu a moderních technologií. Tento fakt jim může vynahradit absenci životních zkušeností. V případě páchání internetových podvodu se tak věk nezdá jako jeden ze zásadních faktorů. Nicméně naopak v případě obětí je věk faktorem naprosto zásadním.

3.6 Oběť internetových podvodů

Je důležité vědět, že oběť trestného činu a poškozený, nemusí být vždy jedna a ta samá osoba. Obětí se může stát pouze fyzická osoba. Poškozeným se může mimo fyzické osoby stát i osoba právnická.[42]

Obětí internetového podvodu se mohou stát jednotlivec nebo také různé organizace. Jejich schopnosti, zkušenosti, a především informovanost v oblasti problematiky kyberprostoru se však mohou výrazně lišit. U těch méně zkušených a informovaných jedinců pochopitelně existuje daleko větší pravděpodobnost, že se stanou obětí této trestné činnosti. Z tohoto hlediska je u jednotlivců nasnadě, že obětí může být ve většině případů pouze senior nebo dítě. Opak je ale pravdou. Ne, že by senioři nebo děti oběťmi pachatelů nebyli, ale obětmi této trestné činnosti se stávají osoby všech věkových kategorií. Z mého pohledu je to dáno především tím, že pachatel věk své oběti většinou nezná. Jemu nejde o věk oběti, ale o její peníze.

3.6.1 Když je obětí jednotlivec

V tomto případě může hrát zásadní roli právě v předešlé podkapitole zmíněný věk oběti. U starších osob, zejména u seniorů existuje větší předpoklad, že pachatel se svým útokem uspěje. Senioři až na výjimky obvykle nejsou v oblasti práce na internetu vzdělaní. Buďto sami nechtějí nebo je pro ně vzdělání v této oblasti hůře dostupné. Stejné to ve většině případů bývá i s prací s výpočetní technikou. Velkým problémem je všeobecné přesvědčení seniorů, že se jich internetové podvody nemohou týkat, neboť

[41] SMEJKAL, V. *Kybernetická kriminalita*, *3. vydání*. Plzeň: Aleš Čeněk, 2022. str. 812.
[42] SVATOŠ, R. *Základy kriminologie a prevence kriminality*. České Budějovice: VŠERS, 2009. s 27.

sami nejsou na internetu aktivní či jsou aktivní úplně minimálně. Ze stejných důvodů jsou ohroženou skupinou také děti. Dnešní děti sice s internetem a moderními technologiemi vyrůstají, nejsou ale tolik vzdělávány v oblasti internetových podvodů. Důvodem může být především fakt, že většina z nich nehospodaří s vlastními finančními prostředky. Rodiče logicky necítí potřebu své děti v této problematice vzdělávat.

U mladší generace lze předpokládat, že s ovládáním výpočetní techniky nemá sebemenší problém. Stejně tak s internetem, který je pro ni naprosto běžnou součástí života. Toto však může být paradoxně příčinou problému, spočívajícím v jejich tvrzení, že se obětí internetového podvodu nemohou stát, neboť s internetem běžně pracují.

Střední generace, též osoby v produktivním věku zase mohou narážet na problémy dnešní uspěchané doby. U této generace je největším nebezpečím nepozornost a neochota věci důkladně prostudovat a pročíst. Lze s nadsázkou říct, že dnes většina z nás kliká a pak až se diví. Mělo by to být ale naopak. Nejprve bychom se měli divit a až poté klikat. Význam této nadsázky spočívá v tom, že by osoby měly v dnešní době klást důraz především na důkladné pročtení textu a jeho porozumění. U spousty případů jsou pachatelé úspěšní právě z důvodu nepozornosti oběti a neochoty číst obsah stránky, na které se nachází.

3.6.2 Když je obětí organizace

Pokud se obětí některého z internetových podvodů stane organizace (společnost, firma), může to mít s ohledem na trh vážný dopad na její další fungování. Z hlediska bezpečnosti stále platí, že nejslabším článkem jsou jednotliví zaměstnanci. Není se mnohdy čemu divit, neboť nízké bezpečnostní povědomí vykazují kolikrát i samotní majitelé organizací či jiní vedoucí pracovníci. Ti si myslí, že je v dnešní době ochrání instalace antivirového programu. Opak je ale pravdou. Způsob, jakým jsou dnes prováděny kybernetické útoky na organizace a jakých slabin je ze strany útočníků při útocích využíváno, jasně ukazuje, že útoky jsou záležitostí zejména sociálního inženýrství.[43] Organizace mají velkou nevýhodu v tom, že jsou z hlediska pachatelů častým terčem. Lze se domnívat, že tomu tak je zejména ze dvou důvodů. Prvním důvodem je to, že organizace většinou disponují velkým množstvím finančních prostředků. O ty jde pachatelům ostatně především. Dalším a pro organizace možná

[43] ŠULC, V. a kolektiv autorů. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018. str. 30-31.

vážnějším důvodem je to, že se pachatelé přímo za organizace či jejich pracovníky mohou vydávat. Následky toho, když se obětí internetového podvodu stane organizace, mohou být velmi závažné.

Mezi následky bude na prvním místě pochopitelně ztráta peněz. Neméně závažnými následky mohou být ztráta důvěry klientů, podání trestního oznámení ze strany klientů, případně trestní stíhání některého ze zaměstnanců, který byť i z nedbalosti pachatelům pomohl. Jmenované následky mohou být pro organizaci až likvidační.

Závěrem lze říct, že organizace čelí a do budoucna budou nadále čelit stále sofistikovanějším internetovým podvodům, které mohou mít závažné finanční a reputační následky. Z hlediska prevence je nezbytné, aby do budoucna investovaly do moderních bezpečnostních opatření a pravidelně školily své zaměstnance, aby byly schopny těmto hrozbám čelit. Pouze tak mohou minimalizovat rizika a chránit své finance, cenné informace a zdroje.

4 Analýza konkrétního způsobu podvodného jednání

V této kapitole hlouběji rozeberu jeden ze způsobů, jakým pachatelé kybernetické trestné činnosti na své oběti útočí. S tímto způsobem podvodu se konkrétně jihočeská policie potýká prakticky každý den. Problém je to ale samozřejmě celorepublikový. Ostatně i to je hlavním důvodem, proč jsem se v této práci rozhodl hlouběji zanalyzovat právě tento způsob. Jedná se o případ fishingu v rámci, kterého se pachatel vydává za falešného bankéře a policistu.

4.1 Popis podvodného jednání

Vše začíná telefonátem, který probíhá velmi profesionálně. Pachatel se nejčastěji vydává za pracovníka České národní banky a následně za pracovníka banky své oběti. Zjištění banky oběti může vypadat asi takto: „Dobrý den, u telefonu Miroslav Šupík, pracuji u České národní banky. V poslední době zaznamenáváme zvýšený počet útoků na bankovní účty. Já se jen pro kontrolu zeptám, u jaké banky máte vedený účet. Výborně, děkuji za spolupráci, za okamžik Vás bude kontaktovat bezpečnostní pracovník Vaší banky. Následuje telefonát, při němž se pachatel již vydává za pracovníka konkrétní banky. Volající „pracovník banky“ se představí, vysvětlí problém (nejčastěji jde o právě probíhající napadení účtu, podezřelou transakci, potvrzení transakce nebo potvrzení žádosti o úvěr) a nabídne tři možnosti jeho řešení.

Prvním z nich je převedení všech peněz na tak zvaný bezpečný účet banky. Tento způsob volí pachatelé asi nejčastěji. Dalším z nabízených řešení je vybrání všech peněz a jejich následné vložení do bitcoinmatu. Posledním, nejméně nabízeným řešením, je možnost připojení se pomocí vzdáleného přístupu do počítače oběti.

Aby pachatel zvýšil uvěřitelnost, používá program, pomocí kterého dokáže skrýt své skutečné telefonní číslo a vydávat ho za jakékoliv existující či také neexistující číslo. Co to je spoofing, jsem vysvětlil v předchozí kapitole. Zkušenosti jsou takové, že si pachatel většinou najde reálné a existující telefonní číslo banky, za jejíhož pracovníka se vydává.

Následuje, není to ale úplně pravidlem, další způsob, pomocí kterého se pachatel snaží zvýšit uvěřitelnost podvodu. V průběhu hovoru oběti sdělí, že napadení účtu již banka oznámila policii, která bude oběť ohledně vzniklého problému kontaktovat.

Kontaktování komplicem, vydávajícím se za policistu, přichází většinou do několika málo minut. Podvodný policista samozřejmě potvrdí tvrzení bankéře a oběti doporučí, aby se řídila jeho dalšími pokyny.

Zde je samozřejmě důležité si uvědomit, že banka za své klienty policii nikdy nic hlásit nebude. V případě, kdy by nějakým způsobem došlo k napadení účtu, k čemuž samozřejmě bez přičinění samotného majitele účtu nemůže dojít, by banka klienta kontaktovala s tím, aby se on sám obrátil na policii. Není možné, aby banka sama za klienta rozhodla, že ho jednání poškozuje natolik, že je nutné, obrátit se na policii.

Pokud však „bankéři“ oslovená osoba uvěří, stává se obětí podvodu a z jejího účtu velice pravděpodobně zmizí leckdy i její celoživotní úspory. Zaznamenány jsou i případy, kdy pachatel oběť vyzve k tomu, aby si za účelem záchrany svého bankovního účtu zjednala úvěr. Pochopitelně oběti zdůrazní, aby o účelu úvěru s nikým v bance nemluvila.

4.1.1 Časový rámec

Pachatel se vždy v tomto případě bude snažit svou oběť zastihnout nepřipravenou. Nelze s jistotou tvrdit, že pachatel tohoto podvodu útočí pouze v ranních, odpoledních nebo večerních hodinách. Pachatel se vždy bude snažit oběť kontaktovat v době, kdy je méně pozorná nebo více důvěřivá. Každý je v tomto ohledu ale jiný. Z tohoto důvodu nelze říct, jaká je pro pachatele ideální doba útoku.

4.1.2 Cílová skupina

Mezi oběťmi tohoto druhu internetového podvodu jsou osoby všech věkových skupin a všech stupňů dosaženého vzdělání. Je to dáno zejména tím, že pachatel ve většině případů nemá o oběti dopředu žádné informace. Nezná pohlaví, věk a samozřejmě ani vzdělání oběti. Jeho cílovou skupinou v tomto případě jistě nebudou nezletilé děti a zkrátka osoby u nichž se lze domnívat, že nemají zřízen bankovní účet.

4.1.3 Dopad na oběti

Dopad na oběti může být v tomto případě velký, zejména s ohledem na finanční stránku. Nejen, že oběť přijde leckdy o všechny své peníze. Ke všemu může splácet také statisícový úvěr, z něhož pro vlastní potřebu nevyužila ani korunu. To může vést k značným problémům z hlediska psychiky. Oběť se může prakticky v jednom okamžiku dostat do finanční tísně a do dluhové pasti. Velkou ránu může utrpět také důvěra. Oběť může být v budoucnu skeptická ohledně důvěry k bankovním institucím, případně k přijímání hovorů z neznámých čísel.

4.2 Jednotlivé kroky podvodného jednání

Podvodné jednání nyní podrobně popíšu bod po bodu, aby bylo jasné, jakým způsobem při něm pachatel postupuje.

1) Prvotní telefonický kontakt pachatele s obětí (většinou za účelem zjištění banky oběti).

2) Pachatel se již vydává za pracovníka konkrétní banky, oběť je informována o problému s jejím bankovním účtem.

3) Pachatel navrhuje oběti jednu z výše popsaných možností řešení problému.

4) Uklidnění oběti, že napadení účtu již řeší policie.

5) Oběti volá pachatel, vydávající se za policistu. Oběti je zdůrazněno, aby se řídila pokyny bankéře.

6) Opětovný kontakt s podvodným bankéřem, který zvoleným způsobem proniká na bankovní účet oběti a okrádá ji o peníze.

4.3 Opatření bankovních institucí

V této kapitole jsem již zmínil, že v České republice nemůže dojít k tomu, aby byl napadnut či prolomen bankovní účet. Vždy k tomu dojde jedině tak, že pachateli nějakým způsobem, byť nevědomě pomůže sám majitel účtu. Dá se říct, že banky mimo finančních

prostředků obchodují také s důvěrou klientů. Banka s nedostatečným zabezpečením účtů klientů, by nejspíše brzy žádné klienty neměla. Vím, že oblast zabezpečení je tou jedinou, kde spolu banky vzájemně spolupracují. Jinak jsou na trhu pochopitelně konkurenty.

V rámci internetových podvodů se ze svých chyb poučují nejen pachatelé, ale také banky, které se samozřejmě snaží peníze svých klientů chránit. Přicházejí tedy s různými preventivními opatřeními. Nejčastější je pravidelná informovanost klientů o aktuálních hrozbách. Klienti jsou informování zejména na webových stránkách bank a pomocí emailu. Neustále se snaží modernizovat a tím posilovat obranu internetového bankovnictví. V neposlední řadě je to zvýšená kontrola podezřelých plateb. Jakmile klient posílá neobvykle vysokou částku na zahraniční účet, je zpravidla kontaktován bankou s tím, zda chce zadanou platbu skutečně provést. Dvoufázové potvrzení plateb je dnes standart již u všech bank. V praxi to vypadá tak, že na mobilní telefon majitele účtu přijde SMS zpráva, která obsahuje unikátní kód. Pokud kód do určitého času nezadáme, transakce je zrušena. I toto však dokáže pachatel pomocí manipulace a ovlivnění oběti překonat.

4.4 Opatření Policie České republiky

Nejúčinnější zbraní Policie České republiky v boji proti všem internetovým podvodům je prevence. O té ale bude řeč až v šesté kapitole. Je potřeba přiznat, že objasněnost internetových podvodů není v rámci republiky nikterak vysoká. Pohybuje se v nižších jednotkách procent. *Není proto náhoda, že boj proti kyberkriminalitě se stal jednou z hlavních priorit Policie České republiky*.[44] Tento cíl si dávala policie už i v minulých letech. Ani letošní rok, tedy rok 2025, nebude výjimkou. Mimo prevence je také důležité, aby měla policie odpovídající počet policistů a vybavení. *V rámci organizační struktury jsou dnes vytvořena specializovaná pracoviště pro boj s internetovou kriminalitou na každém krajském ředitelství policie. Tato pracoviště poskytují ostatním složkám policie odborné znalosti při zajišťování důkazů ze sítě internet.*[45] Dalším důležitým opatřením je, aby se poškození i přes veřejně známou nízkou objasněnost nadále motivovali k tomu, případy napadení jejich účtů oznamovat. Policie se běžně setkává s tím, že poškození nechtějí napadení svých účtů s policií řešit. Jsou

[44] KOŽÍŠEK, M. a PÍSECKÝ, V. *Bezpečně n@ internetu: průvodce chováním ve světě online.* Praha: Grada Publishing, 2016. str. 135.
[45] Tamtéž.

buďto dopředu přesvědčeni, že se nic nevyřeší nebo se jim zkrátka nechce trávit čas na obvodním či místním oddělení. Pro policii je ale každé oznámení důležité. Zejména proto, že se od poškozeného mohou dozvědět nějaký další nový způsob podvodu, proti kterému bude potřeba bojovat. Neméně důležité jsou i telefonní čísla a emaily, ze kterých pachatel oběť kontaktoval.

V předešlé podkapitole zmíněná bankovní opatření společně s opatřeními policie, snad budou mít za následek postupné snižování počtu oznámení internetových podvodů, a naopak zvyšování jejich objasněnosti.

4.5 Závěrečné shrnutí

Tento případ internetového podvodu, ve kterém se pachatelé vydávají za falešné bankéře a policisty, ukazuje, jak sofistikovaná a nebezpečná může moderní kybernetická trestná činnost být. Je nezbytné, aby veřejnost byla informována o těchto typech podvodů a aby byla přijata preventivní opatření k ochraně osobních údajů a financí.

Důležitou roli hraje a bude hrát i do budoucna vzdělávání a osvěta, které mohou pomoci lidem rozpoznat varovné signály a vyhnout se podvodným aktivitám. Klíčovou roli v efektivním boji proti těmto podvodům hraje také spolupráce mezi bankami, policií a dalšími institucemi.

Závěrem je potřeba zdůraznit, že přispět k bezpečnějšímu online prostředí může každý z nás. Stačí, pokud budeme obezřetní a budeme dodržovat základní bezpečnostní pravidla. Tím nejzákladnějším je, že bychom neměli klikat na neznámé odkazy a cokoliv na nich vyplňovat. Tím spíš naše osobní údaje a jakékoliv údaje, týkající se našeho bankovního účtu. Stejně tak bychom tyto údaje neměli sdělovat po telefonu neznámým osobám.

5 Zákony a předpisy týkající se internetových podvodů

V dnešní době, kdy internet hraje velkou roli v našich životech, je důležité chránit se před internetovými podvody. Tato kapitola se zaměřuje na zákony, které nás chrání před různými formami kyberkriminality.

5.1 Zákon o kybernetické bezpečnosti a související předpisy

Během roku 2014 byl schválen zákon o kybernetické bezpečnosti č. 181/2014 Sb., který vstoupil v platnost 1. ledna 2015. Tento zákon stanovuje práva a povinnosti jednotlivců a definuje působnost a pravomoci veřejných orgánů v oblasti kybernetické bezpečnosti. Hlavními důvody pro přijetí zákona byly: 1. rostoucí počet různých forem terorismu, včetně kyberterorismu, a 2. stále větší závislost společnosti a jednotlivců na informačních technologiích. Cílem zákona je vytvořit podmínky pro spolupráci mezi soukromým sektorem a veřejnou správou, aby bylo možné efektivněji řešit incidenty kybernetické bezpečnosti. Zákon také stanovuje práva a povinnosti v této oblasti s cílem zvýšit bezpečnost kybernetického prostoru.[46]

5.1.1 Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích

Vyhláška vstoupila v platnost dne 19. prosince 2014 a zabývá se významnými informačními systémy a kritérii, která je určují. Tato vyhláška nabyla účinnosti od 1. ledna 2015 a stanovuje pravidla a požadavky na zabezpečení těchto systémů, které jsou klíčové pro fungování státu a jeho institucí.[47]

Určující kritéria obsahuje § 3 této vyhlášky. Ve znění paragrafu je uvedeno, jak posuzovat bezpečnost informačních systémů. Kritéria zahrnují možné omezení nebo narušení služeb veřejnosti, hospodaření a fungování orgánů veřejné moci, nebo zásah do osobního života či práv osob. Orgány veřejné moci vedou seznam všech informačních

[46] SMEJKAL, V. *Kybernetická kriminalita*, *3. vydání*. Plzeň: Aleš Čeněk, 2022. str. 159.
[47] SMEJKAL, V., SOKOL, T., KODL, J. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Aleš Čeněk, 2019. str. 33.

systémů, které spravují, a posuzují jejich bezpečnost podle těchto kritérií. Výsledky posouzení zaznamenávají písemně.[48]

5.1.2 Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti

Od 28. května 2018 nahradila nová vyhláška č. 316/2014 Sb. a zapracovala Směrnici NIS. Tato vyhláška se vztahuje na informační systémy kritické infrastruktury, komunikační systémy kritické infrastruktury, významné informační systémy, informační systémy základních služeb a systémy nebo sítě elektronických komunikací používané poskytovateli digitálních služeb.

Vyhláška upravuje:

1) Obsah a strukturu bezpečnostní dokumentace.
2) Obsah a rozsah bezpečnostních opatření.
3) Typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů.
4) Náležitosti a způsob hlášení kybernetických bezpečnostních incidentů.
5) Náležitosti oznámení o provedení reaktivního opatření a jeho výsledku.
6) Vzor oznámení kontaktních údajů a jeho formu.
7) Způsob likvidace dat, provozních údajů, informací a jejich kopií.[49]

5.1.3 Směrnice NIS2

Nová směrnice NIS2 nahrazuje směrnici NIS z roku 2016, která se týká zabezpečení sítí a informací. NIS2 byla schválena v roce 2023 a Česká republika ji musí implementovat do svého právního řádu. V Česku to znamená nahrazení stávajícího zákona o kybernetické bezpečnosti novým, rozsáhlejším zákonem. Tento nový zákon

[48] ČESKO. *Vyhláška č. 317/2014 Sb., §3* [online]. [cit. 18.02.2025]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-317#p3
[49] SMEJKAL, V., SOKOL, T., KODL, J. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Aleš Čeněk, 2019. str. 33-34.

rozšiřuje počet regulovaných odvětví a podniků a zpřísňuje požadavky na kybernetickou bezpečnost. Nově se bude týkat asi 6 000 podniků, zatímco dříve se týkal asi 600. Zákon zavádí dva stupně regulací – nižší a vyšší – podle odvětví a velikosti podniků. Účinnost nového zákona se očekává od poloviny roku 2025, ale závisí na průběhu legislativního procesu. Počet kybernetických incidentů a bezpečnostních hrozeb stále roste. Firmy a organizace jsou stále více závislé na správném fungování svých systémů, kde uchovávají klíčové informace a procesy. Kybernetická bezpečnost se tak stává nezbytnou součástí fungování podniků a klíčových organizací. Proto Evropská unie přišla s novou směrnicí NIS2.[50]

5.2 Vybrané právní předpisy Evropské unie

Také Evropská unie si jistě uvědomuje důležitost zajištění bezpečnosti v oblasti kybernetického bezpečí. I z tohoto důvodu přišla také s vlastními právními předpisy.

5.2.1 Prováděcí nařízení ke směrnici NIS

Dne 31. ledna 2018 vydala Evropská komise prováděcí nařízení (EU) č. 2018/151, které stanovuje pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148 (Směrnice NIS). Toto nařízení upřesňuje bezpečnostní opatření, která musí poskytovatelé digitálních služeb [§ 3 písm. h) podle ZKB] zohlednit při řízení bezpečnostních rizik pro sítě a informační systémy. Dále specifikuje parametry pro posouzení významnosti dopadu incidentu. Nařízení je účinné od 10. května 2018 a je přímo aplikovatelné, což znamená, že je pro poskytovatele digitálních služeb závazné.[51]

5.2.2 Usnesení Evropského parlamentu o boji proti kyberkriminalitě

V tomto usnesení Evropský parlament shrnuje aktuální situaci, protože kyberkriminalita v členských státech roste, a navrhuje opatření v následujících oblastech: prevence, zvýšení odpovědnosti a ručení poskytovatelů služeb, posílení policejní

[50] ČESKO. *Vše o zavádění směrnice NIS2* [online]. [cit. 18.02.2025]. Dostupné z: https://vseonis2.cz/co-je-nis2/
[51] SMEJKAL, V., SOKOL, T., KODL, J. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Aleš Čeněk, 2019, str. 37.

a justiční spolupráce, prosazování právního státu v kyberprostoru, usnadnění získávání elektronických důkazů v trestním řízení. Dále žádá Komisi, aby investovala do IT kapacit a obrany a odolnosti kritické infrastruktury EU, čímž by se snížila zranitelnost EU vůči závažným kybernetickým útokům velkých zločineckých organizací, státem podporovaným útokům nebo teroristickým skupinám. Rovněž se požaduje posílení spolupráce se třetími zeměmi.[52]

5.2.3 Úmluva Rady Evropy o kybernetické kriminalitě

Úmluva o kybernetické kriminalitě má za cíl bojovat proti trestným činům spáchaným pomocí technologií. To zahrnuje situace, kdy jsou technologie jak nástrojem, tak cílem trestného činu, a také případy, kdy technologie podporují jiné trestné činy, jako je například podvod. Úmluva poskytuje pokyny pro tvorbu národních zákonů o počítačové kriminalitě a podporuje mezinárodní spolupráci. Úmluva vznikla na jednání Rady Evropy v Budapešti dne 23. 11. 2001, v platnosti je od 1. 7. 2004.[53]

5.3 Trestní zákoník (zákon č. 40/2009 Sb.)

Trestní zákoník obsahuje samozřejmě hned několik ustanovení, která se zaměřují přímo na boj proti kybernetické kriminalitě. Naprostou většinu těchto trestných činů, nalezneme v trestním zákoníků v hlavě V („Trestné činy proti majetku“).[54] V této podkapitole se zaměřím na dvě nejčastější právní kvalifikace, které policie u internetových podvodů aplikuje.

V současné době je na internetu jedním z nejčastějších protiprávních jednání podvod. Podle trestního zákoníku je podvod definován jako jednání, které má za následek neoprávněné získání majetkové výhody tím, že někdo uvede jiného v omyl nebo využije jeho omylu. V trestním zákoníku ho najdeme pod paragrafem 209.[55]

---

[52] Tamtéž.

[53] EUR-Lex. *Úmluva o počítačové kriminalitě*. Přístup k právu Evropské unie [online]. Dostupné z: https://eur-lex.europa.eu/CS/legal-content/summary/convention-on-cybercrime.html?fromSummary=28

[54] Policie České republiky. *Nejčastější projevy kybernetické kriminality s odkazem na trestní zákoník* [online]. [cit. 19.02.2025]. Dostupné z: https://policie.gov.cz/clanek/nejcastejsi-projevy-kyberneticke-kriminality-s-odkazem-na-trestni-zakonik.aspx

[55] KOŽÍŠEK, M. a PÍSECKÝ, V. *Bezpečně n@ internetu: průvodce chováním ve světě online.* Praha: Grada Publishing, 2016. str. 153.

Pokud někdo podvede jiného a způsobí mu tím škodu na majetku, může být potrestán různými způsoby v závislosti na závažnosti činu. Základní trest je až dva roky vězení, zákaz činnosti nebo propadnutí věci.[56] Trestný čin podvod se týká cizího majetku, což zahrnuje nejen věci, ale také pohledávky a majetková práva. Cizím majetkem je pak nazýváno to, co nepatří pachateli nebo to, co mu patří jen z části.[57]

Trestný čin podvod, je v rámci internetových podvodů nejčastější právní kvalifikací, kterou příslušníci Policie České republiky využívají. V uplynulém roce 2024 bylo v rámci České republiky policií evidováno 15 951 případů podvodu, objasněno bylo celkem 2 350 případů. Celková způsobená škoda činila 16 239 913 korun.[58]

V rámci internetových podvodů se můžeme setkat i s případy, při kterých dojde k neoprávněnému vstupu do počítačového systému, případně k prolomení hesla u některé z internetových služeb.

Pokud někdo neoprávněně získá přístup k počítačovému systému, může být potrestán až dvěma lety vězení, zákazem činnosti nebo propadnutím věci.[59] Tento trestný čin chrání data uložená na nosičích informací před neoprávněným použitím a také počítače nebo jiná telekomunikační zařízení před neoprávněnými zásahy. Nepřímo jsou chráněny i další zájmy, jako jsou obchodní a bankovní tajemství, autorská díla, údaje o pacientech a jiné další informace za předpokladu, že jsou obsaženy na nosiči informací.[60]

V uplynulém roce 2024 bylo v rámci České republiky policií evidováno 1 132 případů neoprávněného přístupu k počítačovému systému a nosiči informací. Pro zajímavost, jihočeská policie do celkového počtu přispěla 57 případy, z nichž se jich 11 podařilo objasnit.[61]

---

[56] KOŽÍŠEK, M. a PÍSECKÝ, V. *Bezpečně n@ internetu: průvodce chováním ve světě online.* Praha: Grada Publishing, 2016. str. 153-154.
[57] JELÍNEK, J. a kolektiv. *Trestní právo hmotné, Obecná část, Zvláštní část, 2. aktualizované vydání.* Praha: Linde Praha a. s., 2006. str. 695.
[58] Policie České republiky, *Statistické přehledy kriminality za rok 2024* [online]. [cit. 06.03.2025]. Dostupné z https://www.policie.gov.cz/clanek/statisticke-prehledy-kriminality-za-rok-2024.aspx.
[59] KOŽÍŠEK, M. a PÍSECKÝ, V. *Bezpečně n@ internetu: průvodce chováním ve světě online.* Praha: Grada Publishing, 2016. str. 160.
[60] JELÍNEK, J. a kolektiv. *Trestní právo hmotné, Obecná část, Zvláštní část, 2. aktualizované vydání.* Praha: Linde Praha a. s., 2006. str. 711-712.
[61] Policie České republiky, *Statistické přehledy kriminality za rok 2024* [online]. [cit. 06.03.2025]. Dostupné z https://www.policie.gov.cz/clanek/statisticke-prehledy-kriminality-za-rok-2024.aspx.

Počítačový systém je zařízení nebo skupina propojených zařízení, která automaticky zpracovávají data podle programu. Patří sem i data uložená, zpracovaná, vyhledaná nebo přenesená těmito zařízeními za účelem jejich provozu, použití, ochrany a údržby.[62]

Ne každá manipulace například s internetovými účty je automaticky výše uvedeným trestným činem. Jako příklad mohu uvést účet na některé ze sociálních sítí. V případě, kdy dojde ne k prolomení, ale pouze k napodobení účtu, nejedná se o trestný čin. Toto tvrzení samozřejmě platí jen v případě, kdy napodobení nebylo součástí nebo pomocí něj nedošlo k spáchání trestné činnosti.

Závěrem této kapitoly lze říct, že zákony týkající se internetových podvodů hrají klíčovou roli v ochraně jednotlivců i organizací před stále sofistikovanějšími hrozbami. S neustálým vývojem technologií můžeme do budoucna jistě očekávat i další legislativní změny, které budou reagovat na nové výzvy v oblasti kybernetické bezpečnosti.

[62] ČESKO. *§ 136a zákona č. 40/2009 Sb., trestní zákoník*.

6 Policie České republiky v boji proti internetovým podvodům

S trestnou činností, která je páchána na internetu se Policie České republiky setkává každý den. I proto pro účely jejího odhalování a vyšetřování vznikají na jednotlivých krajských ředitelstvích k těm stávajícím také nová oddělení. Ta se specializují zejména na kybekriminalitu a boj proti ní. Tato oddělení mohou těm stávajícím poskytovat cenné rady a zároveň je metodicky vést.[63]

Problematika evidování oznámení internetových podvodů není úplně jednoduchá. Příslušník policie, který oznámení přijímá, musí vědět, na co se má osoby podávající trestní oznámení zeptat. Musí být také schopen řádně zajistit případné důkazy. Zejména z tohoto hlediska nemusí být příslušník policie, který je služebně zařazen na obvodním či místním oddělení, mnohdy schopen případ kyberkriminality, zejména internetového podvodu, řádně zaevidovat.

V současné době se tento fakt snaží policie řešit tím, že jsou na každém základním útvaru policie, který tato oznámení přijímá, vybíráni příslušníci, kteří jsou následně v problematice kybernetické kriminality proškolováni. Po úspěšném absolvování školení by tito příslušníci měli mít dostatečné znalosti na to, aby byli schopni přijaté oznámení řádně zaevidovat a následně třeba i ve spolupráci se specializovaným útvarem prověřovat.

6.1 Specializované útvary Policie České republiky

Útvary, specializující se jen na boj proti internetové kriminalitě v dnešní době působí na okresní, krajské i celorepublikové úrovni. Příslušníci těchto útvarů jsou mnohdy právě ti, kteří školí příslušníky základních útvarů policie. Mohou být také autoři metodických pokynů, které řeší právě otázku správného provedení výslechu poškozeného, případně správného zajištění důkazů, aby nedošlo k jejich poškození či jinému znehodnocení pro účely trestního řízení. Začnu tedy od útvaru, jehož působnost je v rámci celé republiky.

[63] KOŽÍŠEK, M. a PÍSECKÝ, V. *Bezpečně n@ internetu: průvodce chováním ve světě online.* Praha: Grada Publishing, 2016. str. 135.

6.1.1 Národní centrála proti terorismu, extremismu a kybernetické kriminalitě

Jedná se o útvar služby kriminální policie a vyšetřování. Vznikl na začátku roku 2023 oddělením dvou sekcí z Národní centrály proti organizovanému zločinu. Hlavním účelem vzniku tohoto útvaru je boj proti terorismu, extremismu a kybernetické kriminalitě. V budoucnu bude potřeba umět těmto výzvám čelit. I proto má tento útvar téměř 170 příslušníků. Prioritou tohoto útvaru je posílení mezinárodní spolupráce v oblasti boje proti kybernetické trestné činnosti. V neposlední řadě je to již mnou zmíněná spolupráce napříč všemi útvary policie.[64]

6.1.2 Odbor analytiky a kybernetické kriminality

Tyto útvary vznikají na jednotlivých krajských ředitelstvích a mají krajskou působnost. Útvar bývá většinou tvořen příslušníky služby kriminální policie a vyšetřování, kteří předtím sloužili na oddělení hospodářské či obecné kriminality. V rámci své činnosti se jak již jeho název napovídá, soustředí především na kybernetickou kriminalitu a metodickou a školící činnost pro příslušníky útvarů nižších instancí. Například mezi útvary jihočeské policie ho však nenajdeme. Pokud není útvar zcela vyčleněn, bývá problematika analytiky a kybernetické kriminality většinou záležitostí oddělení hospodářské kriminality služby kriminální policie a vyšetřování.

6.1.3 Oddělení hospodářské kriminality

Jedná se o útvar služby kriminální policie a vyšetřování, který působí jak na krajské, tak i na okresní úrovni. V případě okresní úrovně řeší především tu trestnou činnost, kterou se ze zákona nemohou zabývat základní útvary policie, tedy obvodní a místní oddělení. Oddělení se zabývá nejen kybernetickou kriminalitou, ale především trestnými činy hospodářskými, které nalezneme v šesté hlavě trestního zákoníku. Další činností je opět metodická, případně školící.

[64] Policie České republiky, *Vznik nového útvaru přispěje k bezpečnosti v ČR i v Evropě* [online]. [cit. 22.02.2025]. Dostupné z https://www.policie.gov.cz/clanek/vznik-noveho-utvaru-prispeje-k-bezpecnosti-v-cr-i-v-evrope.aspx

6.1.4 Obvodní a místní oddělení

Jedná se o základní útvary Policie České republiky. Příslušníci těchto útvarů přicházejí do kontaktu s oznamovateli, poškozenými, ale i s pachateli trestných činů nejvíce. Z hlediska vyšetřování a odhalování internetových podvodů jsou mnohdy těmi nejdůležitějšími. Většinou se totiž poškození a oznamovatelé v případech internetových podvodů obracejí právě na ně. Proto je, jak jsem již zmínil, důležité, aby se jejich příslušníci neustále školili a tím zdokonalovali v oblasti kybernetické kriminality. Pokud bych měl zmínit působnost těchto oddělení z hlediska kyberkriminality, praxe je následovná. Obvodní a místní oddělení mohou řešit zejména ty trestné činy, jejichž horní hranice trestu odnětí svobody nepřevyšuje pět let. V případě trestného činu podvodu, je na základě jednoho z interních aktů řízení policie tou pomyslnou hranicí škoda 100 000 korun. Jakmile tuto hranici škoda přesáhne, případem by se mělo zabývat oddělení hospodářské, případně obecné kriminality služby kriminální policie a vyšetřování.

6.2 Vyšetřování internetových podvodů

Ať už se případem internetového podvodu zabývá obvodní či místní oddělení nebo některý z útvarů služby kriminální policie a vyšetřování, nejdůležitější na jeho objasnění je kvalitní výslech poškozeného. Před výslechem většinou přichází prvotní vytěžení poškozeného. Na základě prvotních informací od poškozeného dojde ke stanovení právní kvalifikace. Ve většině případů se jedná o podvod, tedy § 209 trestního zákoníku. V rámci následného prvotního výslechu by se policie měla zajímat zejména o následující.

- Jakým způsobem došlo k odcizení peněz. O jaký druh internetového podvodu se jednalo.

- Kdo s poškozeným komunikoval, zda to byl cizinec či nikoliv. Pokud to byl cizinec, tak s jakým přízvukem hovořil. Kolik bylo pachatelů.

- Z jakého telefonního čísla a emailu pachatel komunikoval.

- Na jaký účet, případně účty odešly odcizené finanční prostředky.

- Zajištění souhlasu poškozeného s prolomením bankovního tajemství. Na základě tohoto souhlasu dokáže policie ve spolupráci s bankovní institucí poškozeného vyhledat majitele účtu, na který odešly odcizené peníze. Za předpokladu, že se jednalo o účet u české banky.

- Vyžádání kopií emailových či jiných komunikací s pachatelem.

Další velmi důležitou součástí boje policie proti internetovým podvodům je včasné oznámení a ochota poškozeného s policií spolupracovat. V ideálním případě by mělo dojít k oznámení v nejbližší možné době. Ve spoustě případů si poškození uvědomili, že byli podvedeni, prakticky ihned, jakmile z jejich účtu peníze odešli. V případech, kdy si poškození uvědomí podvod ještě v jeho průběhu, případně ihned po něm, měli by okamžitě volat do své banky a vše jí oznámit. Další telefonát by měl poté směřovat na policii.

Ale ani včasné oznámení nebo kvalitně provedený výslech poškozeného, nejsou zárukou toho, že se podaří pachatele dopadnout a poškozenému vrátit jeho peníze. Je potřeba konstatovat, že objasněnost těchto případů je velmi nízká. Pohybuje se skutečně v nižších jednotkách procent. Je to zapříčiněno především sofistikovaností a kvantitou internetových podvodů. O tom ale již v této práci byla řeč.

S ohledem na výše uvedené je největší zbraní policie v boji proti internetový podvodům stále preventivní činnost.

6.3 Preventivní činnost policie

Nejprve je potřeba vysvětlit, co je vlastně prevence. Definicí pojmu prevence bychom našli velké množství. *Autoři kriminologického sborníku definují prevenci kriminality (lat. praeventia–zákrok předem, včasná ochrana, obrana) jako společenská opatření zaměřená na předcházení sociálně patologických jevů ve společnosti, především pak kriminalitě.*[65]

Činnost Policie ČR se nezakládá pouze na represi již nastalého asociálního jednání, ale rozšiřuje se–více než v minulosti-i do oblasti prevence. V současnosti je zcela

[65] SVATOŠ, R. *Prevence kriminality*. České Budějovice: VŠERS, 2014. s 13.

zřejmé, že trvalé snižování kriminality se neobejde bez pečlivé práce při jejím předcházení.[66]

Z hlediska prevence kriminality podle cílové skupiny se Policie České republiky soustředí hlavně na primární prevenci. Cílovou skupinou může být jak široká veřejnost, tak specifické skupiny obyvatel, aniž by se brala v úvahu pravděpodobnost, že se stanou oběťmi trestného činu.[67]

6.3.1 Prevence v oblasti internetových podvodů

Z mého osobního hlediska, je v této oblasti hlavním úkolem prevence informovat veřejnost o nejaktuálnějších trendech v oblasti internetových podvodů. Veřejnost musí vědět, jakým způsobem pachatelé těchto podvodů pracují. Zejména kde a jakým způsobem své oběti oslovují a jakým způsobem s nimi komunikují. Musí se také dozvědět o druzích internetových podvodů, které jsou nejrozšířenější. Tohle vše je úkolem především jednotlivých Oddělení tisku a prevence, která jsou na všech krajských ředitelstvích policie. A jakými způsoby se o to policie vlastně snaží?

6.3.1.1 Přednášky

Nejčastějším způsobem je realizace preventivních přednášek pro veřejnost. Buďto může být přednáška zaměřena konkrétně na určitou skupinu osob (věk, zaměstnanci) nebo na širokou veřejnost. Jak jsem již v této práci zmínil, pachatelé internetových podvodů ve většině případů dopředu neví, jak stará je osoba, se kterou komunikují. Ohroženi jsou tím pádem všichni. Nelze tedy říct, že přednášky jsou vhodné pouze pro seniory.

Velkou výhodou přednášek je osobní kontakt s posluchači. V případě nejasností je tak možné informaci posluchačům zopakovat, případně ji dovysvětlit. Užitečná je také zpětná vazba posluchačů.

[66] Tamtéž, s 73.
[67] SVATOŠ, R. *Základy kriminologie a prevence kriminality*. České Budějovice: VŠERS, 2009. s 38.

6.3.1.2 Využití médií

Každý den se můžeme z médií dozvědět o tom, že v některé části republiky přibyl další poškozený, který chtěl například investovat nebo uvěřil, že má napadený bankovní účet. Práce s médii je doménou především tiskových mluvčích. Z hlediska prevence je tedy velice důležitá také práce tiskových mluvčích. Ti informují širokou veřejnost o internetových podvodech pomocí pravidelných tiskových zpráv a rozhovorů do televizí či rádií. Touto formou se o případu může dozvědět velké množství osob. Ne každý se však dívá na televizní zprávy, poslouchá rádio nebo čte noviny. Nelze se tak spolehnout pouze na média. Je ale důležité, že i přesto, že se případy víceméně opakují, stále vychází v médiích s celorepublikovým dosahem.

6.3.2 Kyber rádce jihočeské policie

Některá krajská ředitelství policie bojují proti internetovým podvodům pomocí vlastního preventivního projektu. Jihočeská policie přišla na počátku roku 2023 s preventivním projektem s názvem Kyber rádce.

Cílem projektu je zvýšit povědomí široké veřejnosti o nejaktuálnějších trendech v oblasti internetových podvodů a zároveň poskytnout rady, jak se obětí podvodu nestát. Projekt je realizován nejčastěji formou přednášek pro veřejnost. S projektem je možné se potkat také například v některém z nákupních center, kde je realizován formou kontaktního terénního pracoviště.[68]

Když policisté tento projekt zakládali, denně v rámci Jihočeského kraje evidovali 4-5 případů internetových podvodů. Nutno říct, že čísla nejen v Jihočeském kraji nikterak neklesají.

Proč tomu tak je, a co by bylo dobré v tomto ohledu zlepšit, řeší praktická část této práce.

[68] Policie České republiky, *KYBER RÁDCE jihočeské policie* [online]. [cit. 23.02.2025]. Dostupné z https://www.policie.gov.cz/clanek/kyber-radce-jihoceske-policie.aspx

7 Praktická část

Poslední část bakalářské práce se věnuje praktické části, kde na základě výzkumného šetření, které bylo koncipováno kvalitativně, za použití metody dotazování, a to technikou řízených rozhovorů u osob z každé věkové skupiny – nezletilý, mladistvý, dospělý, senior. Bylo zjišťováno, zda je informovanost veřejnosti ohledně internetových podvodů ze strany Policie České republiky dostatečná.

7.1 Cíl výzkumu

Hlavním cílem výzkumu bylo zhodnotit efektivitu a metody informování veřejnosti o internetových podvodech ze strany Policie České republiky, včetně preventivních kampaní a dostupnosti informačních zdrojů. Vedlejším cílem bylo navrhnout doporučení ke zlepšení informovanosti veřejnosti s cílem zvýšit povědomí o rizicích a prevenci internetových podvodů.

7.2 Výzkumné otázky

1. Jak často se setkáváte s informacemi o internetových podvodech od Policie České republiky?
2. Víte, jaké jsou nejčastější typy internetových podvodů, na které Policie České republiky upozorňuje?
3. Znáte preventivní opatření, která Policie České republiky doporučuje k ochraně před internetovými podvody?
4. Využíváte nějaké z těchto preventivních opatření ve svém každodenním životě? Pokud ano, které?
5. Jak hodnotíte dostupnost a srozumitelnost informací o internetových podvodech poskytovaných Policií České republiky?
6. Setkali jste se někdy s internetovým podvodem? Pokud ano, věděli jste, jak postupovat a kam se obrátit?

7. Jaké komunikační kanály (např. webové stránky, sociální sítě, tiskové zprávy) považujete za nejefektivnější pro šíření informací o internetových podvodech?

8. Máte nějaké návrhy na zlepšení informovanosti veřejnosti o internetových podvodech ze strany Policie České republiky?

7.3 Metodika

7.3.1 Metodika sběru dat

Výzkumné šetření bylo koncipováno kvalitativně, kdy byla použita metoda dotazování a to technikou řízených rozhovorů. Rozhovory byly realizovány u osob z každé věkové skupiny.

7.3.2 Technika sběru dat

Byla použita technika sběru dat pomocí polostrukturovaných řízených rozhovorů, s přesně modifikovanými otázkami k informovanosti veřejnosti o internetových podvodech ze strany Policie České republiky, viz. Příloha bakalářské práce.

7.3.3 Výzkumný soubor

Výzkumné šetření se uskutečnilo ve Městě Prachatice. Prachatice mají 11 250 obyvatel a jsou okresním městem. Leží v Jihočeském kraji, zhruba 45 kilometrů od Českých Budějovic.

Každou věkovou skupinu ve výzkumném souboru zastupoval jeden jedinec: nezletilý, mladistvý, dospělý a senior.

7.3.4 Realizace výzkumu a analýza dat

Výzkum byl realizován od 1. do 7. března 2025. Analýza dat byla provedena od 8. do 10. března 2025.

7.3.5 Etika výzkumu

Všichni účastníci byli informováni o tématu a cíli výzkumu. Byli také ujištěni, že veškeré získané informace budou použity výhradně pro účely tohoto výzkumu a jejich anonymita bude zachována. Jména účastníků nejsou nikde uvedena. Výzkum byl proveden v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů.

7.4 Výsledky výzkumu

Ze všech odpovědí na položené výzkumné otázky, bylo analýzou, komparací a hodnocením těchto výsledků zjištěno, že informovanost veřejnosti ohledně internetových podvodů není všeobecně na špatné úrovni. Je to samozřejmě o tom, že ten, koho toto téma zajímá, si o něm informace bude vyhledávat častěji. U nezletilého, mladistvého a dospělého bylo zjištěno, že se s informacemi o podvodech setkávají zejména na sociálních sítích. Zástupce seniorů informace čerpá víceméně pouze z tisku a televize. Znalost konkrétních typů podvodů byla různorodá. U mladších ročníků byla značně ovlivněná sociálními sítěmi. Starší ze zástupců disponovali zejména znalostmi podvodů, týkajících se bankovních účtů. Dotázaní vesměs znali základní preventivní doporučení policie. Lze říct, že každý si pochopitelně pamatuje a řídí se jen těmi opatřeními, které se týkají oblasti, ve které se nejčastěji pohybují. S podvodem ze všech zástupců nesetkal pouze nezletilý. S ohledem na to, že nezletilí nejsou cílovou skupinou pachatelů, není toto zjištění žádným překvapením. Dle očekávání bylo zjištěno, že mladší ročníky tíhnou spíše k sociálním sítím a z hlediska informování veřejnosti je považují za nejefektivnější metodu. Představovali by si na nich ze strany policie větší aktivitu. Dospělý a senior by zase ocenili větší aktivitu policie z hlediska pořádání informačních besed.

Jediné základní východisko pro výzkumné šetření této bakalářské práce, byl polostrukturovaný řízený rozhovor, s přesně modifikovanými otázkami k zjištění míry informovanosti veřejnosti ohledně internetových podvodů ze strany Policie České republiky.

Jednotlivé rozhovory jsou součástí přílohy této bakalářské práce. Souhrnné výsledky na výzkumné otázky (dále jen „VO“) všech dotázaných jsou následující:

Na VO 1 - Jak často se setkáváte s informacemi o internetových podvodech od Policie České republiky?

Z výsledků výzkumného šetření bylo zjištěno, že se dotázaní o internetových podvodech dozvídají víceméně pravidelně, i když z různých zdrojů. Mladší část dotázaných sbírá informace výhradně na sociálních sítích, starší část vyjma sociálních sítí a internetu také z hromadných sdělovacích prostředků.

Na VO 2 - Víte, jaké jsou nejčastější typy internetových podvodů, na které Policie České republiky upozorňuje?

Zástupce nezletilých měl informace o podvodech souvisejících se sociálními sítěmi. Mladistvý zase disponoval informacemi o podvodech, které vesměs cílí na osobní údaje. Podle očekávání měli největší přehled oba starší zástupci, kteří byli dobře informováni zejména ohledně podvodů, jejichž cílem jsou bankovní účty.

Na VO 3 - Znáte preventivní opatření, která Policie České republiky doporučuje k ochraně před internetovými podvody?

U všech dotázaných se projevila znalost zejména těch nejzákladnějších preventivních opatření. Zmiňováno bylo především zodpovědné zacházení s osobními údaji a opatrnost ohledně otevírání neznámých emailů a otevírání odkazů v nich.

Na VO 4 - Využíváte nějaké z těchto preventivních opatření ve svém každodenním životě? Pokud ano, které?

Všichni dotázaní víceméně shodně uvedli, že neotvírají neznámé odkazy.

Na VO 5 - Jak hodnotíte dostupnost a srozumitelnost informací o internetových podvodech poskytovaných Policií České republiky?

Dotázaní považovali poskytované informace ze strany Policie České republiky vesměs za srozumitelné. Názory na jejich dostupnost se různily. Ti mladší by si představovali větší využití sociálních sítí. Dospělý hodnotil dostupnost spíše z hlediska zájmu o téma jako takovém. Senior by si představoval větší pozornost pro jeho věkovou kategorii.

Na VO 6 - Setkali jste se někdy s internetovým podvodem? Pokud ano, věděli jste, jak postupovat a kam se obrátit?

Vyjma zástupce nezletilých se s internetovým podvodem setkali již všichni zbylí dotázaní. Jednalo se o podezřelé emaily a podvod v rámci prodeje zboží na internetu. Jak postupovat v případě, kdy by se stali obětí podvodu, věděli všichni.

Na VO 7 - Jaké komunikační kanály (např. webové stránky, sociální sítě, tiskové zprávy) považujete za nejefektivnější pro šíření informací o internetových podvodech?

Vyjma zástupce seniorů panovala u všech shoda, že nejefektivnějším nástrojem budou v současné době zejména sociální sítě. Zástupce seniorů považoval za nejefektivnější nástroj stále televizi a rádio.

Na VO 8 - Máte nějaké návrhy na zlepšení informovanosti veřejnosti o internetových podvodech ze strany Policie České republiky?

Opět panovala mezi dotázanými shoda na tom, že by bylo ze strany Policie České republiky dobré, zaměřit se více na sociální sítě. Zmíněn byl návrh na spolupráci s youtubery, případně známými influencery, kteří jsou v dnešní době veřejností hojně sledovaní. Zástupce z řad seniorů si představoval větší aktivitu v oblasti pořádání preventivních přednášek.

8 Diskuze

Tato práce byla zaměřena na internetové podvody a roli Policie České republiky v informování veřejnosti o těchto hrozbách. S kybernetickou trestnou činností se v České republice potýkáme již od 90. let 20. století. V té době se internet začínal stávat běžnou součástí životů lidí. Policie České republiky začala trestnou činnost v kyberprostoru podrobně sledovat v roce 2011. Od té doby počty případů této trestné činnosti neustále rostou. Největší zlom však nastal v době pandemie onemocnění Covid19.

Kybernetická trestná činnost, zejména internetové podvody se postupem času vyvíjely a neustále zdokonalovaly. V současné době je sofistikovanost a zejména kvantita internetových podvodů na takové úrovni, že se v různých podobách mohou týkat nás všech. Buďto se můžeme přímo stát cílem útočníka, nebo se tím cílem může stát někdo v našem okolí.

Role Policie České republiky je v boji s internetovými podvody naprosto klíčová, zejména pak její preventivní činnost. Efektivní informování široké veřejnosti může výrazně snížit počet obětí podvodů. Šíření informací o způsobu, jakým pachatelé na své oběti útočí může přispět také k vytvoření bezpečnějšího online prostředí pro všechny jeho uživatele. Z tohoto důvodu jsem si za cíle této bakalářské práce zvolil zhodnocení míry informovanosti veřejnosti ohledně internetových podvodů ze strany Policie České republiky a také navržení doporučení ke zlepšení informovanosti veřejnosti s cílem zvýšit povědomí o rizicích a prevenci internetových podvodů.

Výsledky výzkumu ukázaly, že informovanost veřejnosti o internetových podvodech je na dobré úrovni, nicméně stále jsou zde mezery, které by bylo dobré zaplnit. Je důležité uznat, že míra informovanosti veřejnosti o internetových podvodech závisí především na jejím zájmu a ochotě se v této oblasti vzdělávat. Pokud ze strany veřejnosti nebude zájem, informovanost zůstane pořád stejná. S neustálým vývojem této trestné činnosti bude časem dokonce klesat.

Jedním z klíčových zjištění je, že většina respondentů si je vědoma základních typů internetových podvodů a mají informace, jakým způsobem se zachovat v případě, kdy by se stali obětí, případně by byli ze strany pachatele osloveni. Lze se domnívat, že toto povědomí je do značné míry výsledkem aktivní informační kampaně

Policie České republiky. Nicméně, navzdory těmto snahám, stále existuje značná část populace, která není dostatečně informována o preventivních opatřeních a správném postupu v případě, kdy se stanou obětí podvodu. Ostatně toto potvrzují i neklesající počty oznámení.

Dalším důležitým zjištěním je, že efektivita informačních kampaní může být zvýšena cílením na specifické věkové skupiny. Například nezletilí a mladiství preferují informace šířené prostřednictvím sociálních sítí, zatímco starší generace dávají přednost tradičním médiím, jako jsou televize, tisk či rádio. Tento rozdíl v preferencích naznačuje, že Policie České republiky by měla přizpůsobit své komunikační strategie tak, aby efektivně oslovila všechny demografické skupiny.

Na základě informací, které jsem v rámci výzkumu získal, navrhuji následující zlepšení v oblasti informování veřejnosti. V případě prevence internetových podvodu bude do budoucna potřeba, zaměřit se na jednotlivé věkové kategorie zvlášť.

V práci je již zmíněno, že nezletilé osoby nebývají primárními cíli pachatelů, ve většině případů totiž nedisponují vlastními finančními prostředky a nemají ani vlastní bankovní účty. Mohou být ale skrz ně zranitelní všechny zbývající věkové kategorie jakožto jejich rodinný příslušníci. U nezletilých je potřeba, zaměřit se především na práci s osobními údaji. Musí vědět, jak se svými osobními údaji zacházet. Kam je zadávat, kam ne. Je naprosto klíčově, aby věděli, že osobní údaje v rukou nesprávného člověka mohou být velice nebezpečné. Navrhuji preventivní přednášky zaměřené primárně na práci s osobními údaji. Nemusí se jednat o klasické přednášky. Je potřeba dosáhnout toho, aby téma posluchače bavilo a naplňovalo. Tohoto výsledku lze dosáhnout za pomoci moderních technologií. Přednášky lze pojmout interaktivně, případně formou hry. Posluchače by v tomto případě bylo dobré rozdělit na skupiny a na každý úkol jim dát určený časový limit. Doporučuji také, obrátit se na youtubery a influencery, kteří jsou nezletilými hojně sledováni.

Mladistvé osoby tráví většinu času na sociálních sítích. Zde navrhuji, primárně se zaměřit především na ně. Stejně jako u nezletilých navrhuji oslovit youtubery a influencery, kteří by v rámci svých videí mohli varovat na nebezpečnost internetových podvodů. Samotné téma by ale pro sledující nemuselo být až tak zajímavé. Navrhuji jít cestou toho, že by oslovení v rámci svých běžných témat na konci každého videa či

podcastu přidali nějakou z preventivních rad. Tím dosáhneme toho, že se informace k posluchačům a sledujícím dostanou.

U dospělých navrhuji větší využití sociálních sítí. Zde již můžeme vytvářet příspěvky a natáčet videa či podcasty, které budou přímo hovořit o problematice internetových podvodů. Přednášky na toto téma policie již realizuje, nicméně je potřeba se zaměřit na jejich propagaci. K tomu by mohly posloužit právě sociální sítě. Navrhuji zaměřit se na spolupráci se známými osobnostmi, které by policie mohla oslovit z důvodu spolupráce při natáčení preventivních videí a spotů na toto téma. Odbodnou taktiku využívá policie v současné době v rámci náborových kampaní. Navrhuji vytvoření krátkých televizních reklamních spotů, které budou varovat před internetovými podvody. Stejně tak natočení podcastu, které se bude tomuto tématu věnovat v rádiích.

U seniorů navrhuji stejná televizní a rádiová opatření, jako u dospělých. Přednášky by se však daly pojmout zábavnější formou. Navrhuji vytvoření divadelních představení, kde by jednotlivé scénky humornou formou varovaly před jednotlivými druhy internetových podvodů. V rámci klasických přednášek by mohla být policie více proaktivní a s tématem navštěvovat domovy a kluby seniorů.

Závěr

Tato bakalářská práce se zajímala o internetové podvody a roli Policie České republiky v informování veřejnosti.

V práci zmiňuji historii kybernetické kriminality, nicméně v současné době je důležité, dívat se do budoucna. Internetové podvody prošli za pomoci moderních technologií velkým zdokonalením. Jejich sofistikovanost je v současní době již na takové úrovni, že jim může podlehnout téměř každý. Věk či stupeň dosaženého vzdělání zde již nehrají žádnou roli. Ještě nebezpečnější se jeví kvantita internetových podvodů. I díky rozvoji sociálních sítí mohou pachatelé naráz v rámci jednoho útoku oslovit obrovské množství lidí. Zejména z tohoto důvodu je v boji proto nim naprosto klíčová role Policie České republiky, která s pachateli internetových podvodů denně bojuje. Vypátrání a dopadení pachatelů této trestné činnosti je bohužel velice těžké. Největší zbraní policie je tak prevence, kterou bude do budoucna nutné rozvíjet a podporovat ji.

Hlavním cílem bakalářské práce bylo posoudit typy internetových podvodů a jejich četnost na území České republiky s důrazem na aktuální hrozby. Zde jsem se zaměřil nejprve na historii a následně na představení internetových podvodů jako takových. Přestaveny byly nejvyužívanější metody internetových podvodníků a také byli detailně popsány konkrétní druhy internetových podvodů, se kterými se Policie České republiky denně potýká. Zmíněna byla také důležitost Policie České republiky v boji proti internetovým podvodům. Zaměřil jsem se na specializované a také základní útvary Policie České republiky, jejichž příslušníci internetové podvody denně evidují a následně vyšetřují. V neposlední řadě byla představena preventivní činnost policie, jejíž důležitost je v současné době větší než kdy dřív.

Práce ukázala, jak jsou internetové podvody dnešní doby ze strany pachatelů propracované a mnohdy dotažené téměř do dokonalosti. Odhalit podvodné jednání je víceméně otázkou nešikovnosti pachatele, než šikovností a znalostmi široké veřejnosti. Úspěch, případně neúspěch pachatele se mnohdy skrývá v opravdu malém detailu. Do budoucna je potřeba počítat s tím, že internetových podvodů bude nadále přibývat a lze se domnívat, že jejich úroveň bude nadále stoupat. Pachatelům v tomto případě dost pomáhají a pomáhat budou i nadále dnešní moderní technologie. Je potřeba počítat s tím,

že pachatelé budou využívat také umělou inteligenci, s pomocí níž zase dokáží rozšířit svou síť a oslovit naráz ještě větší množství osob.

Další částí této bakalářské práce byla praktická část, která se týkala výzkumného šetření, které bylo koncipováno kvalitativně, za použití metody dotazování, technikou řízených rozhovorů se zástupcem s každé věkové skupiny nezletilý, mladistvý, dospělý a senior.

Tímto výzkumným šetřením jsem se pokusil splnit i vedlejší cíle bakalářské práce, kde byla nejprve posouzena otázka efektivity a metod informování veřejnosti o internetových podvodech ze strany Policie České republiky, včetně preventivních kampaní a dostupnosti informačních zdrojů. Poté jsem přistoupil k navržení doporučení ke zlepšení informovanosti veřejnosti s cílem zvýšit povědomí o rizicích a prevenci internetových podvodů.

Z výzkumného šetření vyplynulo, že základní informovanost veřejnosti není na špatné úrovni. Oslovení respondenti disponovali základními znalostmi ohledně prevence a věděli, jak se zachovat v případě, kdyby se stali obětí podvodu. Znalosti se pochopitelně lišily s ohledem na věk. Stejně tak návrhy na zlepšení informovanosti ze strany Policie České republiky. Mladší ročníky preferovaly sociální sítě, ti starší dávali stále přednost tradičním hromadným informačním prostředkům.

Na základě zjištěných informací jsem navrhnul zaměřit se a posílit spolupráci v oblasti sociálních sítí. Bylo by dobré, pokusit se navázat spolupráci zejména s youtubery a influencery, kteří mají značný vliv na dnešní mládež. Dále by bylo dobré, přehodnotit strategii vedení a propagace preventivních přednášek. Přednášky by mohly být pojaté interaktivní formou, která by posluchače více bavila a na přednášky by přitáhla více lidí. K propagaci by se více měli využívat média. Myslím tím zejména regionální, případně oblastní televize a rádia. Další možností je z přednášek udělat divadelní představení, v rámci kterých by se informace o internetových podvodech široké veřejnosti předávaly zábavnou formou. Myslím si, že realizace těchto doporučení může mít za následek kvalitnější a efektivnější informování veřejnosti.

Domnívám se, že stanovené cíle bakalářské práce byly splněny.

Seznam použitých zdrojů

Literární zdroje

1. BEDNÁŘ, V. *Internetová publicistika*, *Žurnalistika a komunikace*. Praha: Grada Publishing, 2011. 216 s. ISBN 978-80-247-3452-1.

2. BROOKSHEAR, J. Glenn. *Informatika.* Brno: Computer Press, 2013. 608 s. ISBN 978-80-251-3805-2.

3. JELÍNEK, J. a kolektiv. *Trestní právo hmotné, Obecná část, Zvláštní část, 2. aktualizované vydání.* Praha: Linde Praha a. s., 2006. 823 s. ISBN 80-7201-630-X.

4. JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada Publishing, 2007. 284 s. ISBN 978-80-247-1561-2.

5. KOHOUT, R., KLOZOVÁ, M. *Internetem bezpečně (nejen) pro seniory*. Karlovy Vary: you connected, 2020. 55 s. ISBN 978-80-907852-0-5.

6. KOLOUCH, J., BAŠTA, P., KROPÁČKOVÁ, A. a KUNC, M. *CyberSecurity*. Praha: CZ.NIC, 2019. 560 s. ISBN 978-80-88168-31-7.

7. KOŽÍŠEK, M. a PÍSECKÝ, V. *Bezpečně n@ internetu: průvodce chováním ve světě online.* Praha: Grada Publishing, 2016. 176 s. ISBN 978-80-271-9074-4.

8. MATEJKA, J. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praha: CZ.NIC, 2013. 256 s. ISBN 978-80-904248-7-6.

9. SMEJKAL, V., SOKOL, T., KODL, J. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Aleš Čeněk, 2019. 378 s. ISBN 978-80-7380-765-8.

10. SMEJKAL, V. *Kybernetická kriminalita*, *3. vydání*. Plzeň: Aleš Čeněk, 2022. 1166 s. ISBN 978-80-7380-849-5.

11. STRAUS, J., PORADA, V. a kolektiv. *Teorie, metody a metodologie kriminalistiky*. Plzeň: Aleš Čeněk, 2017. 417 s. ISBN 978-80-7380-666-8.

12. SVATOŠ, R. *Prevence kriminality*. České Budějovice: VŠERS, 2014. 132 s. ISBN 978-80-87472-76-7.

13. SVATOŠ, R. *Základy kriminologie a prevence kriminality*. České Budějovice: VŠERS, 2009. 118 s. ISBN 978-80-86708-81-2.

14. ŠALMON, T. *(Ne)bezpečný internet, Sprievodca pre používateľov internetu od 10 do 99 rokov*. Bratislava: Lindeni, 2021. 292 s. ISBN 978-80-566-1941-4.

15. ŠULC, V. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018. 148 s. ISBN 978-80-7380-737-5.

16. ŠULC, V. a kolektiv autorů. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech*. Praha: Policejní akademie České republiky, 2020. 328 s. ISBN 978-80-7251-505-9.

Internetové zdroje

1. Policie České republiky. *Kyberkriminalita* [online]. [cit. 11.02.2025]. Dostupné z: https://policie.gov.cz/clanek/kyberkriminalita.aspx

2. Policie České republiky. *Jednotlivé druhy kyberkriminality* [online]. [cit. 13.02.2025]. Dostupné z: https://policie.gov.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

3. Policie České republiky. *Pomoc obětem TČ, Počítačová kriminalita* [online]. [cit. 13.02.2025]. Dostupné z: https://policie.gov.cz/clanek/pomoc-obetem-tc-pocitacova-kriminalita.aspx

4. Policie České republiky. *Preventivní informace, Smishing* [online]. [cit. 14.02.2025]. Dostupné z: https://policie.gov.cz/clanek/preventivni-informace-smishing.aspx

5. Policie České republiky. *nePINdej* [online]. [cit. 14.02.2025]. Dostupné online z: https://policie.gov.cz/clanek/nepindej.aspx

6. Policie České republiky. *Vývoj registrované kriminality v roce 2024* [online]. [cit. 14.02.2025]. Dostupné z: https://policie.gov.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2024.aspx

7. Policie České republiky. *Současné trendy podvodníků – vishing a spoofing* [online]. [cit. 09.01.2025]. Dostupné z: https://policie.gov.cz/clanek/prevence-rady-a-doporuceni-soucasne-trendy-podvodniku-vishing-a-spoofing.aspx

8. Policie České republiky. *Smishing* [online]. [cit. 09.01.2025]. Dostupné z: https://policie.gov.cz/clanek/smishing.aspx

9. ČESKO. *Vše o zavádění směrnice NIS2* [online]. [cit. 18.02.2025]. Dostupné z: https://vseonis2.cz/co-je-nis2/

10. EUR-Lex. *Úmluva o počítačové kriminalitě*. Přístup k právu Evropské unie [online]. Dostupné z: https://eur-lex.europa.eu/CS/legal-content/summary/convention-on-cybercrime.html?fromSummary=28

11. Policie České republiky. *Nejčastější projevy kybernetické kriminality s odkazem na trestní zákoník* [online]. [cit. 19.02.2025]. Dostupné z: https://policie.gov.cz/clanek/nejcastejsi-projevy-kyberneticke-kriminality-s-odkazem-na-trestni-zakonik.aspx

12. Policie České republiky, *Statistické přehledy kriminality za rok 2024* [online]. [cit. 06.03.2025]. Dostupné z https://www.policie.gov.cz/clanek/statisticke-prehledy-kriminality-za-rok-2024.aspx.

13. Policie České republiky, *Vznik nového útvaru přispěje k bezpečnosti v ČR i v Evropě* [online]. [cit. 22.02.2025]. Dostupné z https://www.policie.gov.cz/clanek/vznik-noveho-utvaru-prispeje-k-bezpecnosti-v-cr-i-v-evrope.aspx

14. Policie České republiky, *KYBER RÁDCE jihočeské policie* [online]. [cit. 23.02.2025]. Dostupné z https://www.policie.gov.cz/clanek/kyber-radce-jihoceske-policie.aspx

Legislativní dokumenty

1. ČESKO. *§ 217 zákona č. 40/2009 Sb., trestní zákoník*. In: Zákony pro lidi.cz [online]. © AION CS 2010–2025 [cit. 21. 2. 2025]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40#p217

2. ČESKO. *Vyhláška č. 317/2014 Sb., §3* [online]. [cit. 18.02.2025]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-317#p3

3. ČESKO. *§ 136a zákona č. 40/2009 Sb., trestní zákoník*.

Seznam obrázků

Přílohy

Rozhovor 1: Žák 8. třídy základní školy, který miluje hraní online her a sledování videí na YouTube. Rád objevuje nové věci na internetu.

1. Jak často se setkáváte s informacemi o internetových podvodech od Policie České republiky?

Občas vidím nějaké informace na internetu nebo slyším o tom ve škole, když nám učitelé říkají, jak se chovat na sociálních sítích.

2. Víte, jaké jsou nejčastější typy internetových podvodů, na které Policie České republiky upozorňuje?

Ano, slyšel jsem o podvodech na sociálních sítích, kde se někdo vydává za někoho jiného.

3. Znáte preventivní opatření, která Policie České republiky doporučuje k ochraně před internetovými podvody?

Ve škole nám policista při přednášce říkal, že bychom neměli sdílet své osobní údaje s cizími lidmi, měli bychom používat silná hesla a být opatrní při klikání na neznámé odkazy.

4. Využíváte nějaké z těchto preventivních opatření ve svém každodenním životě? Pokud ano, které?

Ano, snažím se používat silná hesla a neklikat na podezřelé odkazy.

5. Jak hodnotíte dostupnost a srozumitelnost informací o internetových podvodech poskytovaných Policií České republiky?

Myslím, že informace jsou docela srozumitelné, ale někdy je těžké je najít. Bylo by fajn, kdyby byly více viditelné na sociálních sítích.

6. Setkali jste se někdy s internetovým podvodem? Pokud ano, věděli jste, jak postupovat a kam se obrátit?

S podvodem jsem se nesetkal, ale kdyby se to stalo, řekl bych to rodičům nebo učitelům a oni by mi pomohli.

7. Jaké komunikační kanály (např. webové stránky, sociální sítě, tiskové zprávy) považujete za nejefektivnější pro šíření informací o internetových podvodech?

Myslím, že sociální sítě jsou nejlepší, protože tam trávíme hodně času. Také by bylo dobré mít informace na školních webových stránkách nebo v aplikacích, které používáme.

8. Máte nějaké návrhy na zlepšení informovanosti veřejnosti o internetových podvodech ze strany Policie České republiky?

Bylo by fajn, využívat více sociální sítě. Také by mohli dělat více přednášek ve školách

Rozhovor 2: Student střední školy, který tráví hodně času na sociálních sítích, jako jsou Instagram a TikTok. Je velmi společenský a rád sdílí své zážitky s přáteli, ale někdy podceňuje rizika spojená s online sdílením osobních informací.

1. Jak často se setkáváte s informacemi o internetových podvodech od Policie České republiky?

Informace o internetových podvodech vidím poměrně často, hlavně na sociálních sítích a někdy i ve škole, když máme přednášky o bezpečnosti na internetu.

2. Víte, jaké jsou nejčastější typy internetových podvodů, na které Policie České republiky upozorňuje?

Ano, vím o případech, kdy se někdo snaží získat naše osobní údaje, a také o podvodech na falešných e-shopech a podvodech při prodeji a koupi zboží.

3. Znáte preventivní opatření, která Policie České republiky doporučuje k ochraně před internetovými podvody?

Ano, doporučují nepoužívat stejné heslo pro více účtů, neklikat na podezřelé odkazy, ověřovat si pravost e-shopů a být opatrný při sdílení osobních údajů.

4. Využíváte nějaké z těchto preventivních opatření ve svém každodenním životě? Pokud ano, které?

Ano, neklikám na podezřelé odkazy a vždy si ověřuji pravost e-shopů, než na nich něco nakoupím.

5. Jak hodnotíte dostupnost a srozumitelnost informací o internetových podvodech poskytovaných Policií České republiky?

Informace jsou docela dostupné a srozumitelné, ale myslím, že by mohly být více propagované na sociálních sítích a na YouTube.

6. Setkali jste se někdy s internetovým podvodem? Pokud ano, věděli jste, jak postupovat a kam se obrátit?

Ano, jednou jsem dostal podezřelý e-mail, ale věděl jsem, že nemám klikat na přiložené odkazy. Kdyby se něco stalo, věděl bych, že mám kontaktovat policii.

7. Jaké komunikační kanály (např. webové stránky, sociální sítě, tiskové zprávy) považujete za nejefektivnější pro šíření informací o internetových podvodech?

Myslím, že sociální sítě jsou nejefektivnější.

8. Máte nějaké návrhy na zlepšení informovanosti veřejnosti o internetových podvodech ze strany Policie České republiky?

Bylo by fajn, kdyby policie dělala více videí a příspěvků na sociálních sítích, které by byly zaměřené na mladé lidi. Také by mohli zapojit influencery, aby šířili informace.

Rozhovor 3: IT specialista, který pracuje v korporaci. Je technicky zdatný a dobře si uvědomuje rizika spojená s kybernetickou bezpečností. Snaží se chránit své osobní i pracovní údaje, ale někdy se setkává s novými typy podvodů, které ho mohou překvapit.

1. Jak často se setkáváte s informacemi o internetových podvodech od Policie České republiky?

Informace o internetových podvodech od Policie České republiky vídám poměrně často, zejména na sociálních sítích a na internetu, kde se téměř každý den objeví nový případ. O podvodech se mluví ve všech sdělovacích prostředcích.

2. Víte, jaké jsou nejčastější typy internetových podvodů, na které Policie České republiky upozorňuje?

Ano, jsem si vědom nejčastějších typů internetových podvodů. Hodně se mluví o podvodech v rámci investování a napadení bankovního účtu.

3. Znáte preventivní opatření, která Policie České republiky doporučuje k ochraně před internetovými podvody?

Ano, nevyplňovat osobní údaje na podezřelých odkazech, ověřovat pravost webových stránek a nepřipojovat se na nezabezpečené wifi připojení.

4. Využíváte nějaké z těchto preventivních opatření ve svém každodenním životě? Pokud ano, které?

Používám silná hesla, ověřuji si webové stránky a neklikám na podezřelé odkazy.

5. Jak hodnotíte dostupnost a srozumitelnost informací o internetových podvodech poskytovaných Policií České republiky?

Informace jsou dostupné a srozumitelné. Problém je spíš v tom, že se o to lidi moc nezajímají. Myslí si, že se jich to netýká.

6. Setkali jste se někdy s internetovým podvodem? Pokud ano, věděli jste, jak postupovat a kam se obrátit?

Ano, při prodeji zboží. Ozval se mi podvodník, který si chtěl pro zboží poslat kurýra. O podvodu jsem ale věděl, takže jsem komunikaci hned ukončil.

7. Jaké komunikační kanály (např. webové stránky, sociální sítě, tiskové zprávy) považujete za nejefektivnější pro šíření informací o internetových podvodech?

V současné době budou nejefektivnější asi sociální sítě. Je na nich každý, už i někteří senioři.

8. Máte nějaké návrhy na zlepšení informovanosti veřejnosti o internetových podvodech ze strany Policie České republiky?

Bylo by užitečné, kdyby policie dělala více videí a příspěvků na sociálních sítích, které by byly zaměřené na různé věkové skupiny. Také by mohli dělat více přednášek a seminářů pro veřejnost.

Rozhovor 4: Důchodce, který často komunikuje s rodinou a přáteli přes e-mail a sociální sítě. I když se snaží být opatrný, někdy je pro něj těžké rozpoznat podvodné e-maily a webové stránky. Často hledá rady od svých vnoučat, jak se chránit online.

1. Jak často se setkáváte s informacemi o internetových podvodech od Policie České republiky?

Informace o internetových podvodech vídám v novinách nebo o nich slyším v televizi. Někdy také dostávám od banky e-maily s varováními.

2. Víte, jaké jsou nejčastější typy internetových podvodů, na které Policie České republiky upozorňuje?

Často slyším o podvodech, kdy se někdo vydává za banku nebo jinou instituci.

3. Znáte preventivní opatření, která Policie České republiky doporučuje k ochraně před internetovými podvody?

Ano, doporučují nepoužívat stejné heslo pro více účtů, neklikat na podezřelé odkazy, ověřovat si pravost internetových stránek a být opatrný při sdílení osobních údajů.

4. Využíváte nějaké z těchto preventivních opatření ve svém každodenním životě? Pokud ano, které?

Se vším mi pomáhá rodina, takže se nemusím tolik starat. Mám ale silná hesla a neotvírám cizí e-maily.

5. Jak hodnotíte dostupnost a srozumitelnost informací o internetových podvodech poskytovaných Policií České republiky?

Informace by mohly být dostupnější pro starší lidi. Zejména pro ty, kteří nemusí být tak zdatní v používání internetu.

6. Setkali jste se někdy s internetovým podvodem? Pokud ano, věděli jste, jak postupovat a kam se obrátit?

Ano, jednou jsem dostal podezřelý e-mail, ale věděl jsem, že nemám klikat na odkazy. Od té doby cizí emaily ani neotvírám. Volal jsem to dceři. Na policii jsem se neobrátil.

7. Jaké komunikační kanály (např. webové stránky, sociální sítě, tiskové zprávy) považujete za nejefektivnější pro šíření informací o internetových podvodech?

Myslím, že by bylo dobré zaměřit se na televizi a rádio. Teď jsou moderní ty sociální sítě, ale spousta lidí, které znám, je nemají a mít nejspíš ani nebudou.

8. Máte nějaké návrhy na zlepšení informovanosti veřejnosti o internetových podvodech ze strany Policie České republiky?

Bylo by užitečné, kdyby policie dělala více kampaní zaměřených na starší lidi, například prostřednictvím televize a rádia. Také by mohli pořádat semináře a přednášky pro seniory, aby se dozvěděli více o tom, jak se chránit.