

POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra managementu a informatiky

Bezpečnost platebního styku v České republice

BAKALÁŘSKÁ PRÁCE

Security of the payment system in the Czech Republic

Bachelor thesis

VEDOUCÍ PRÁCE

Ing. Jan URBANEC

AUTOR PRÁCE

Jiří MAŇÁSEK

PRAHA

2024

Čestné prohlášení

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

V Praze, dne 14. 3. 2024

Jiří MAŇÁSEK

Poděkování

Chtěl bych poděkovat svému vedoucímu panu Ing. Janu Urbancovi za odborné rady, vedení a vstřícnost při konzultacích mé bakalářské práce.

Anotace

Tato bakalářská práce se zabývá tématem bezpečnosti platebního styku. V první části je zpracována charakteristika a základní pojmy, týkající se této problematiky. Druhá část seznamuje čtenáře s podvodným jednáním a riziky, kterým jsou klienti a banky vystaveny. Třetí část je zaměřena na reakci státu a dalších subjektů na bezpečnostní hrozby v oblasti platebního styku. Poslední část tvoří praktická část bakalářské práce, která zkoumá edukaci veřejnosti v rámci financí a její bezpečnosti. Cílem výzkumu, který je tvořen formou dotazníkové ankety, bylo získání dat o preferencích platebního styku a znalostech rizik s tím spojených.

Klíčová slova

Platební styk, podvody, bezpečnost plateb, finance, kyberkriminalita, osobní údaje

Anotation

This bachelor thesis addresses the topic of payment security. The first part provides an overview and basic concepts related to this issue. The second part introduces the reader to fraudulent behavior and risks faced by both clients and banks. The third part is focused on the response of the state and other entities to security threats in the area of payment systems. The last part consists of the practical part of the bachelor thesis, which examines the education of the public within the framework of finance and its security. The aim of the research, conducted in the form of a survey, was to gather data on payment preferences and knowledge of associated risks.

Key words

Payment system, frauds, payment security, finances, cybercrime, personal data

Obsah

Úvod.....	6
1 Charakteristika platebního styku	8
1.1 Platební styk hotovostní	10
1.2 Platební styk bezhotovostní	11
2 Podvody a rizika platebního styku.....	14
2.1 Padělání bankovek a mincí	14
2.2 Phishing	15
2.3 Sextortion phishing	16
2.4 SMiShing	16
2.5 Vishing	18
2.6 Investiční podvody	19
2.7 Skimming	20
2.8 Libanonská smyčka a zadržení hotovosti	21
2.9 Praní špinavých peněz.....	21
2.10 Podvody spojené s kryptoměnou	22
2.11 Love fraud.....	22
2.12 Podvod s nigerijským princem	22
3 Ochrana platebního styku	24
3.1 Právní úprava	24
3.2 Česká národní banka.....	27
3.3 Finanční analytický úřad	29
3.4 Finanční arbitř	29
3.5 Ochrana bankovek a mincí	31
3.6 Ochrana platebních karet.....	33
3.7 Ochrana internetového bankovníctví.....	34
4 Praktická část.....	36
4.1 Výsledky dotazníkového šetření	37
Závěr.....	50
Seznam použité literatury.....	53
Seznam grafů a tabulek	57
Přílohy.....	58

Úvod

V moderní době se bankovníctví neustále vyvíjí a přizpůsobuje novým technologiím a trendům. Jedním z nejvýraznějších posunů je rostoucí trend využívání bezhotovostních platebních metod, které se stávají nedílnou součástí každodenního života. Tento fenomén je důsledkem rychlého rozvoje digitálních technologií a zvýšeného důrazu na pohodlí a efektivitu platebních operací.

S rostoucím využíváním platebních karet, internetového bankovníctví a mobilních platebních aplikací se otevírá nový rozměr platebního styku, který nabízí uživatelům širší možnosti a flexibilitu při provádění finančních transakcí. Avšak s tímto rozvojem přichází i nová rizika a výzvy v oblasti bezpečnosti platebního styku. S narůstajícím počtem online transakcí roste i počet potenciálních hrozeb spojených s kyberkriminalitou a podvody. Bezpečnost platebního styku se tak stává jedním z klíčových témat nejen pro finanční instituce, ale i pro jednotlivce a podniky.

Cílem mé bakalářské práce je zhodnocení bezpečnosti platebního styku v České republice, analýza nejčastějších hrozeb a následná reakce subjektů na tyto hrozby. V první části bakalářské práce se budu zabývat rozdělením platebního styku podle různých kritérií a definováním klíčových pojmů. Porozumění těmto aspektům platebního styku je základem pro pochopení bezpečnostních rizik spojených s každým typem platební operace. Tímto způsobem se přiblížíme k analýze konkrétních bezpečnostních hrozeb a podvodů, které mohou ohrozit platební styk jednotlivců i institucí. Největšími moderními hrozbami jsou phishing a vishing, které spoléhají na manipulativní techniky a neinformovanost jednotlivců. Bakalářská práce se bude detailně zabývat mechanismy, jež útočníci využívají v těchto i jiných typech podvodů. Identifikace rizik je důležitá pro prevenci a vytvoření účinných strategií k boji proti této formě trestné činnosti.

Poslední kapitola teoretické části bude obsahovat opatření a instituce, která Česká republika zavedla, aby posílila bezpečnost platebního styku a minimalizovala rizika v oblasti finančních podvodů.

Součástí této bakalářské práce bude praktická část, která se metodou kvantitativního dotazníkového šetření zaměří na povědomí veřejnosti o bezpečnosti platebního styku. Toto šetření bude sloužit k získání důležitých

informací o preferencích a znalostech respondentů v oblasti financí a bezpečnosti platebních operací. Cílem dotazníkového šetření je porozumět postojům a chování respondentů vůči různým platebním metodám, jejich povědomí o bezpečnostních hrozbách spojených s platebním stykem a úroveň důvěry v bezpečnostní opatření poskytovaná finančními institucemi. Znalosti a preference jednotlivců v této oblasti jsou klíčové pro úspěšnou prevenci platebních podvodů a zabezpečení platebního prostředí pro všechny uživatele.

Analýza výsledků tohoto šetření poskytne poznatky o aktuálním stavu povědomí a chování veřejnosti v oblasti bezpečnosti platebních operací. Tímto způsobem se bakalářská práce zaměří na individuální roli a zodpovědnost každého jednotlivce a na důležitost vzdělávání a osvěty v oblasti bezpečnosti platebního styku.

1 Charakteristika platebního styku

Krátká historie

Platby provázejí lidstvo již od pradávných dob, kdy se začaly vyvíjet první formy směnného obchodu. Lidé vyměňovali zboží a služby přímo, bez využití měny. Poté ve starověku vznikly první mince, což znamenalo přechod od barterového obchodu k využití peněz (Šenkýřová, str. 12-14, 1997)¹. Během raného středověku se v Číně objevily papírové peníze a ve vrcholném středověku byly v Evropě založeny první banky a bankovní účty. Od novověku se začaly používat bankovky a došlo k rozšíření šeků, které se staly běžným nástrojem pro usnadnění transakcí. Od 20. století můžeme využívat kreditní karty, elektronické platební metody a internetové bankovníctví (Eisenhammerová, str. 9, 2014)². S nástupem chytrých telefonů se staly mobilní platby běžným způsobem transakcí. Stejně tak se objevily kryptoměny, které spustily nový druh decentralizovaných digitálních plateb.

Vymezení pojmů

Platební služby – platební služby jsou klíčovým prvkem ekonomiky, umožňují obchod a tok financí. Je to soubor finančních produktů a transakčních mechanismů, které umožňují jednotlivcům, firmám a institucím provádět platby, převody peněz a uskutečňovat další finanční operace. Banky a některé další instituce nabízejí tyto služby na základě povolení České národní banky. (Zdroj: Česká bankovní asociace).

Řadíme mezi ně například:

- Vložení nebo výběr hotovosti z účtu
- Převod financí
- Informace o platebním účtu
- Správa platebního účtu

¹ ŠENKÝŘOVÁ, Bohuslava. *Bankovníctví*. Praha: Grada, 1997. ISBN 80-716-9464-9.

² EISENHAMMEROVÁ, Monika a HEMŽSKÁ, Andrea. *Platební styk: studijní opora*. Pardubice: Univerzita Pardubice, 2014. ISBN 978-80-7395-869-5.

Platební styk – platební styk je nedílnou součástí našeho života. Přestože ho každý den využíváme, je potřeba si vymezit konkrétní definici. „Platební styk je peněžní vztah mezi plátcem a příjemcem, který je uskutečněný v určitých formách dohodnutými platebními instrumenty buď přímo mezi nimi, nebo prostřednictvím k tomu určených subjektů (např. bank nebo spořitelních a úvěrních družstev)“ (Schlossberger, 2012, str. 11)³. Nutno podotknout, že platební styk zahrnuje větší škálu právních vztahů mezi subjekty, na rozdíl od platebních služeb, které poskytují pouze vybrané platební instrumenty.

Druhy platebního styku (Schlossberger, 2012)⁴

Podle způsobu placení

- hotovostní
- bezhotovostní

Podle území

- vnitrostátní
- přeshraniční
- zahraniční

Dle průvodních dokumentů

- dokumentární platební styk
- nedokumentární platební styk

Dle lhůty k vykonání

- expresní (přednostní)
- standardní

Vztah banky k převodu

- závazkový
- bezzávazkový

³ SCHLOSSBERGER, Otakar. *Platební služby*. Praha: Management Press, 2012. ISBN 978-80-7261-238-3.

⁴ SCHLOSSBERGER, Otakar. *Platební služby*. Praha: Management Press, 2012. ISBN 978-80-7261-238-3.

1.1 Platební styk hotovostní

Hotovostní platební styk představuje formu transakcí, kde platby probíhají v podobě fyzických peněz – bankovek a mincí. Hotovostní platební styk stojí na jednoduchém principu – fyzická přítomnost peněz. Bezpečně uložené v peněžence nebo kapse, peníze přecházejí z ruky do ruky. Platby jsou okamžité. Zákazník předává přesně tolik, kolik chce zaplatit, a transakce je uzavřena. Zároveň jsou tyto platby široce přijímány téměř všude. Nemají omezení spojená s technologickými systémy nebo bankovními účty. Jelikož hotovostní platby nejsou spojeny s konkrétním účtem, poskytují relativně vysokou úroveň anonymity a soukromí. Bankovky a mince jsou do oběhu vydávány Českou národní bankou (ČNB), která má za cíl stabilní fungování finančního systému (Máče, 2006)⁵.

Mince

Mince mají různé nominální hodnoty, například 1 Kč, 2 Kč, 5 Kč, 10 Kč, 20 Kč a 50 Kč. Každá hodnota reprezentuje určitou částku v korunách. Mince jsou obvykle vyrobeny z různých kovů a slitin, včetně mědi, niklu, hliníku a mosazi. Každá mince má specifický design, který může obsahovat portréty významných osobností, historické symboly nebo kulturní motivy, ovšem na lící straně těchto mincí je vyražen český lev. V České republice se mince razí v Jablonci nad Nisou.

Bankovky

Stejně jako mince, i bankovky mají různé nominální hodnoty. V České republice jsou bankovky v hodnotách 100 Kč, 200 Kč, 500 Kč, 1000 Kč, 2000 Kč a 5000 Kč. Každá bankovka má specifickou velikost, barvu a design. Na lící straně jsou znázorněny známé osobnosti české historie, jako například Karel IV., František Palacký nebo Ema Destinová. Autorem grafické stránky českých bankovek je akademický malíř Oldřich Kulhánec (ČNB).

⁵ MÁČE, Miroslav. *Platební styk: klasický a elektronický*. Praha: Grada, 2006. ISBN 80-247-1725-5.

1.2 Platební styk bezhotovostní

Bezhotovostní platební styk zahrnuje transakce, při kterých není fyzicky přenášena hotovost. Místo toho jsou platby uskutečňovány elektronickými prostředky. Z tohoto způsobu platby plyne několik výhod jak pro spotřebitele, tak i pro podniky a banky. Kreditní a debetní karty jsou častým prostředkem bezhotovostního platebního styku. Spotřebitelé mohou provádět transakce jednoduše zasunutím nebo přiložením karty k platebnímu terminálu. S rozvojem internetu a digitálních technologií se stále více platebních transakcí uskutečňuje online prostřednictvím internetového bankovníctví. Spotřebitelé mohou provádět platby, spravovat účty a převádět peníze elektronicky. Také využívání mobilních zařízení pro uskutečňování plateb stále nabývá na popularitě. Mobilní platby mohou být prováděny pomocí platebních aplikací, jako jsou Apple Pay nebo Google Pay. Mezi další bezhotovostní platby můžeme zařadit faktury a inkaso, ty mohou být rovněž uskutečňovány elektronicky, což usnadňuje správu plateb a snižuje riziko chyb spojených s manuálním zpracováním papírových dokumentů (Schlossberger, 2012)⁶.

Platební služby

V této podkapitole bych rád věnoval pozornost nejčastěji používaným platebním službám. Zde si jednoduše popíšeme jednotlivé služby, k čemu slouží a v jaké formě existují. V další kapitole si vysvětlíme rizika a protiprávní jednání s nimi spojená.

Debetní karty: Tyto karty jsou připojeny k bankovnímu účtu držitele a platby jsou prováděny přímo z jeho účtu. Peníze jsou okamžitě odečteny při provedení transakce. Debetní karty umožňují držitelům přístup k prostředkům na jejich účtech a také poskytují možnost výběru hotovosti z bankomatů. V současné době jsou debetní karty standardní výbavou téměř každého běžného účtu.

⁶ SCHLOSSBERGER, Otakar. *Platební služby*. Praha: Management Press, 2012. ISBN 978-80-7261-238-3.

Kreditní karty: Umožňují držitelům provádět platby na základě půjčených peněz od vydavatele karty. Platby se obvykle provádějí do výše sjednaného úvěrového rámce. Držitelé mají možnost splatit celý dluh bez úroku, pokud nepřekročí bezúročné období.⁷

Internetové bankovníctví: Jedná se o službu poskytovanou bankami a finančními institucemi, která umožňuje klientům spravovat své bankovní účty a provádět různé finanční transakce prostřednictvím internetu. Díky internetovému bankovníctví mají klienti přístup k jejich bankovním účtům a dalším finančním produktům z pohodlí jejich domova nebo jakéhokoli místa, kde je možné připojení k internetu. Klient tak získá přehled o svých bankovních účtech, včetně aktuálního zůstatku, transakční historie a detailu jednotlivých transakcí. Dále může provádět platby, převádět peníze na různé účty, či platit faktury. Jednou z velkých výhod je správa veškerých finančních produktů, kterými klient disponuje, například obsluha spořicího účtu, kreditní karty, hypotéky nebo investic.

Mobilní platby: Tato služba stojí na technologii NFC (Near Field Communication), která označuje bezdrátovou komunikaci mezi zařízeními jako jsou mobilní telefony, tablety, platební terminály, chytré hodinky či karty a další. Uživatelé musí nejprve nastavit mobilní platební aplikaci na svém chytrém telefonu. To obvykle zahrnuje propojení karty nebo bankovního účtu s aplikací a ověření identity. Následně vybere, zda chce provést platbu pomocí elektronické peněženky (například Apple Pay, Google Pay) nebo platební aplikace poskytované bankou⁸. Poté stačí chytré zařízení přiložit k platebnímu terminálu nebo jinému chytrému zařízení a transakce je hotova. Mít platební kartu v mobilu nebo hodinkách je nejen pohodlné, ale i bezpečné. Citlivé údaje z karty se totiž v zařízeních neukládají a jsou nahrazeny náhodně generovaným autentizačním kódem.

⁷ EISENHAMMEROVÁ, Monika a HEMŽSKÁ, Andrea. *Platební styk: studijní opora*. Pardubice: Univerzita Pardubice, 2014. ISBN 978-80-7395-869-5.

⁸ *Co je NFC platba?* Online. Moneta. 2023. Dostupné z: <https://www.moneta.cz/slovník-pojmu/detail/co-je-nfc-platba>. [cit. 2024-03-06].

Elektronické peněženky: Elektronické peněženky jsou webové nebo mobilní aplikace, které lze používat k placení na internetu. Nejčastějším příkladem elektronické peněženky jsou PayPal, Apple Pay nebo Google Pay. V Česku se nejčastěji jedná o GoPay⁹.

Kryptoměny: Kryptoměna je digitální měna, která je založena na kryptografických technologiích a funguje na základě decentralizovaného systému, nazývaného blockchain. Kryptoměny nejsou fyzické, jako tradiční peníze, ale jsou uchovávány a vyměňovány elektronicky. Nejznámější kryptoměnou je Bitcoin, ale existuje mnoho dalších, včetně Ethereum, Litecoin a mnoha dalších. Kryptoměny jsou využívány jako forma investice a jsou především známy svou vysokou volatilitou, což z nich dělá atraktivní a zároveň riskantní investiční nástroj.

Platební terminály: Jedná se o elektronické zařízení, které umožňuje přijímání plateb kartou v obchodech nebo restauracích. Platba probíhá přiložením nebo vložením karty do platebního terminálu. K platebnímu terminálu lze přiložit i mobilní telefon či chytré hodinky, které podporují funkce bezkontaktního placení.

Šeky: Šek je finanční nástroj, který slouží k provádění platby. Je to kus papíru, který obsahuje pokyn bankovní instituci vyplatit určitou částku peněz z účtu držitele šeku na jiný účet nebo na hotovost. Šeky jsou často používány k provádění platby za zboží nebo služby, ale mohou být také použity pro jiné účely, jako je převod peněz nebo darování peněz. Mezi náležitosti šeku patří: vystavující, příjemce, částka, která má být vyplacena, datum vystavení a bankovní informace¹⁰. Jedná se o starší metodu bezhotovostního styku, která je v poslední době nahrazována modernějšími platebními metodami. V současné době se převážně používají k PR (Public relations) akcím, jako je předávání peněz zvířecím útulkům, dětskému domovu nebo pro boj s rakovinou.

⁹ *Elektronická peněženka*. Online. Komerční banka. 2022. Dostupné z: <https://www.kb.cz/cs/podpora/slovník/vyrazy-zacinajici-na-e/elektronicka-penezenka#:~:text=Elektronick%C3%A1%20pen%C4%9B%C5%BEnka%20je%20webov%C3%A1%20nebo,pomoc%C3%AD%20e%2Dmailu%20a%20hesla.> [cit. 2024-03-06].

¹⁰ MÁČE, Miroslav. *Platební styk: klasický a elektronický*. Praha: Grada, 2006. ISBN 80-247-1725-5.

2 Podvody a rizika platebního styku

V této kapitole se zaměřím na nejčastější podvody, které se mohou týkat platebního styku. Tato trestná činnost může vážně narušit finanční stabilitu na různých úrovních, od jednotlivců a firem až po celé ekonomiky. Většina z těchto podvodů může přímo vést ke ztrátě peněz, což má negativní dopad na finanční stabilitu postižených subjektů. Oběti těchto praktik mají poté oslabenou důvěru v obchodní prostředí.

2.1 Padělání bankovek a mincí

Padělání bankovek a mincí bylo vždy považováno za těžký zločin. Cílem je vytvářet falešné kopie peněz s úmyslem oklamat obchodníky, spotřebitele a finanční instituce. Tato forma podvodu má dlouhou historii, od ručního kopírování mincí po sofistikovanější metody, které se vyvinuly s rozvojem tisku a digitálních technologií. Podle M. Fryštáka pachatelům také napomáhá fakt, že jednotlivci, kteří pracují s penězi, často nejsou dostatečně seznámeni s touto problematikou. Vliv padělání peněz na ekonomiku je značný. Falešné peníze mohou způsobit devaluaci měny¹¹. Kvůli mezinárodní povaze finančních trhů je důležitá spolupráce mezi zeměmi. Centrální banky, vlády a mezinárodní organizace spolupracují na výměně informací a zajišťují opatření, která mají chránit měny před padělateli.

Tabulka č.1 – Padělané a pozměněné bankovky a mince

	2022	2023
Celkem	1 120	3 539
• z oběhu	973	2 927
• před oběhem	147	612

Zdroj: *Padělky 2023 Padělané a pozměněné bankovky a mince zadržené na území ČR*. Česká národní banka.

¹¹ *Trestné činy proti měně de lege lata a de lege ferenda*. Marek Fryšták, Eva Žatecká. 2010.

V roce 2023 došlo k nárůstu zadržení padělaných a pozměněných bankovek oproti předchozímu roku. Zatímco v roce 2022 bylo zadrženo celkem 1120 padělaných bankovek a mincí, v roce 2023 se tento počet téměř ztrojnásobil, dosahujíc čísla 3539 kusů. Dle vyjádření České národní banky, padělané a pozměněné bankovky či mince bývají zpravidla nekvalitního provedení a jejich kvalita je nízká. Při manipulaci s těmito penězi je nezbytné věnovat pozornost bezpečnostním prvkům, aby bylo možné padělek odhalit¹².

2.2 Phishing

Slovo phishing je odvozeno z anglického „fishing“, které znamená „rybařit“, což v tomto kontextu označuje rozesílání „návnady“ v naději, že se některé oběti „chyty“¹³.

Phishing je forma kybernetického útoku, při kterém se útočník snaží získat citlivé informace od jednotlivců nebo organizací tím, že se vydává za důvěryhodnou instituci nebo osobu. Typicky se phishingový útok provádí prostřednictvím falešných e-mailů, webových stránek nebo sociálních sítí.

Útočník si vytvoří falešnou identitu, která se zdánlivě jeví jako důvěryhodná. Může se jednat o konkrétní banku, doručovací službu nebo webovou stránku (sociální síť). Poté z této falešné identity začne rozesílat e-maily, které na první pohled vypadají jako oficiální. Tyto zprávy zpravidla odkazují na falešné webové stránky nebo obsahují přílohy s malwarem. Falešné zprávy často obsahují naléhavé výzvy k akci, které mají přimět oběť k okamžité odpovědi, například změně hesla, potvrzení účtu nebo zadání osobních údajů. Phishingové zprávy často využívají psychologických triků, aby získaly důvěru a vzbudily strach, zvědavost nebo dojem naléhavosti¹⁴.

¹² *Padělky 2023 Padělané a pozměněné bankovky a mince zadržené na území ČR.* Online.

Česká národní banka. 2024. Dostupné

z: https://www.cnb.cz/export/sites/cnb/cs/verejnost/.galleries/pro_media/konference_projevy/vystoupeni_projevy/download/kubelkova_20240304_padelky_2023.pdf. [cit. 2024-03-06].

¹³ *What is phishing?* Online. IBM. 2023. Dostupné z: <https://www.ibm.com/topics/phishing>. [cit. 2024-03-06].

¹⁴ *Počítačová kriminalita.* Online. Policie České republiky. 2020. Dostupné

z: <https://www.policie.cz/clanek/pomoc-obetem-tc-pocitacova-kriminalita.aspx>. [cit. 2024-03-06].

Obětí podvodného jednání se stal například muž z Českokrumlovska, který obdržel e-mail s autorizací přijetí finanční částky na bankovním účtu. Použil odkaz z e-mailu a byl přesměrován na známou internetovou stránku své banky, kde zadal osobní údaje. Vzápětí zjistil, že z jeho účtu odcházely částky ve výši několika desítek tisíc korun. Odkaz byl samozřejmě podvodný a vedl na falešné stránky banky, aby z oběti vylákal údaje. Tyto údaje následně pachatel využil a začal čerpat finance z účtu oběti¹⁵.

2.3 Sextortion phishing

Jedná se o formu kybernetického podvodu, která zahrnuje vydírání jednotlivce pomocí kompromitujících materiálů. Podvodník musí jako první získat přístup do e-mailové schránky, aby ukázal, že má kontrolu nad soukromím oběti (například pomocí „brute force“ techniky generování hesel). Poté odešle e-mail vlastníkově e-mailové schránky s tím, že má kompromitující materiály oběti a nebojí se je zveřejnit. Nezveřejní je pouze v případě, že mu je zaslána určitá částka v kryptoměnách. Tento typ podvodu není tak známý a rozšířený, jelikož zpravidla vyžaduje přístup k e-mailové schránce oběti, na rozdíl od klasického phishingu, který lze pouze rozeslat na různé adresy¹⁶. Příklad sextortion phishingové zprávy lze najít v Příloze č. 1.

2.4 SMiShing

Smishing je zkratka pro slovní spojení "SMS phishing" a představuje formu kybernetického útoku, při kterém útočníci využívají textových zpráv (SMS) k podvodu jednotlivců a získání citlivých informací. Tento typ útoku využívá podobné taktiky jako e-mailový phishing.

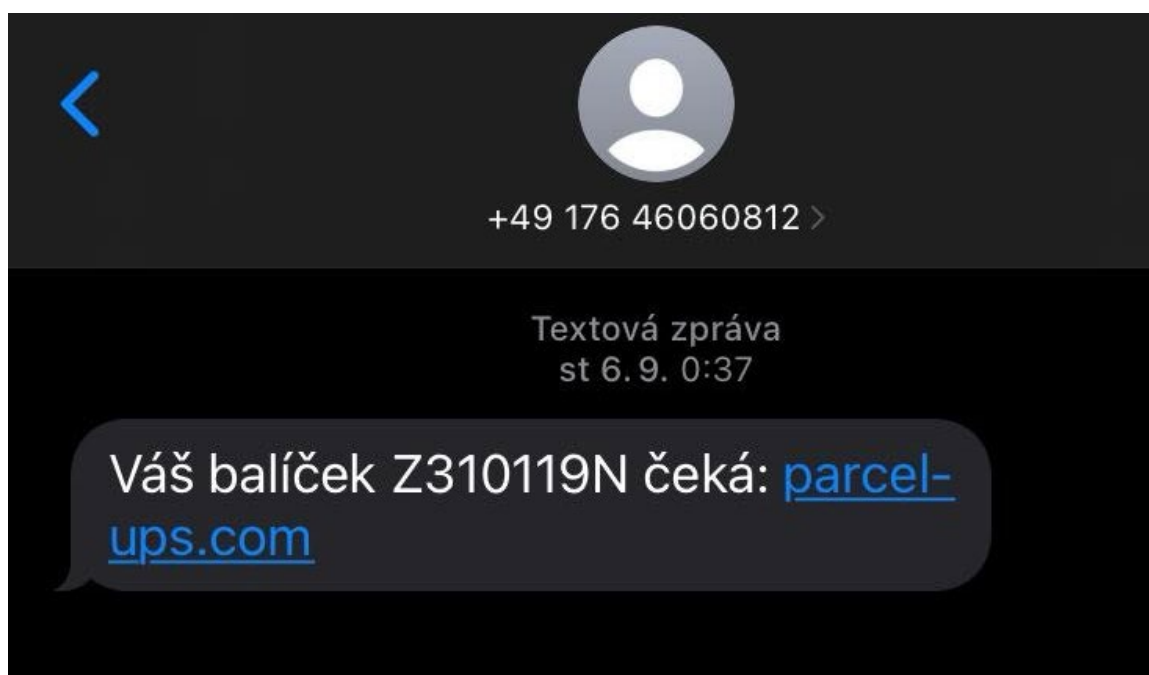
Útočník si vytvoří falešnou identitu, nebo se vydává za důvěryhodnou společnost v textových zprávách. Nejčastěji banky, doručovací služby nebo mobilní operátoři. Zprávy obsahují zavádějící nebo naléhavé informace s cílem nalákat oběť k

¹⁵ *Stal se obětí podvodného e-mailového útoku. Přišel o desítky tisíc.* Online. Prachatický deník.cz. 2021. Dostupné z: <https://prachaticky.denik.cz/zlociny-a-soudy/stal-se-obeti-podvodneho-e-mailoveho-utoku-prisel-o-desitky-tisic-20210310.html>. [cit. 2024-03-06].

¹⁶ *Sextortion emails: how to protect yourself.* Online. National cyber security center. 2018. Dostupné z: <https://www.ncsc.gov.uk/guidance/sextortion-scams-how-to-protect-yourself>. [cit. 2024-03-07].

podvodu. Může se jednat o oznámení o falešné transakci, varování o možném útoku nebo nabídku, která nutí oběť k okamžité reakci. Často obsahují odkazy vedoucí na falešné webové stránky, které imitují oficiální stránky institucí. Tyto stránky mají za cíl získat citlivé informace od oběti. Smishing je nebezpečný hlavně tím, že cílí na uživatele mobilních zařízení prostřednictvím textových zpráv, což zvyšuje pravděpodobnost okamžité reakce¹⁷.

Obrázek č. 1 – SMiShingová zpráva



Zdroj: vlastní tvorba

V tomto příkladě smishingu můžeme vidět, že útočník vytvořil falešnou identitu a falešnou webovou stránku, která připomíná zahraniční doručovací službu UPS. V textové zprávě je oběť vylákána na webovou stránku, aby zde zadala osobní údaje.

¹⁷ Co je smishing. Online. Moneta. 2019. Dostupné z: <https://www.moneta.cz/slovník-pojmu/detail/smishing>. [cit. 2024-03-07].

2.5 Vishing

Vishing je jedním z útoků sociálního inženýrství, ovšem tento je prováděn přes telefonát. Odtud také pochází název podvodu – vishing je zkratkou pro „Voice phishing“.

Volající se snaží získat k osobním údajům nebo k jiným citlivým informacím oběti, aby je poté mohl využít k jinému trestnému činu. Cílem je obvykle získání přístupu k bankovnímu účtu.

Při vishingových útocích se pachatel spoléhá na sociální normy a lidský instinkt. Může se vydávat za policistu, pracovníka úřadů nebo bankéře. V oběti může hovor s důvěryhodnou autoritou vzbudit nervozitu, zvědavost nebo povinnost odpovědět. Podvodníci využívají těchto emocí, a ještě je posílí pomocí hrozeb a různých psychologických taktik¹⁸. Podle policejního prezidia České republiky, bývají tvrzení podvodníků velmi věrohodná. Předem si zjistí u jaké instituce má jejich oběť účet a telefonní číslo, kterým ji kontaktují napodobí, aby bylo identické telefonnímu číslu dané instituce. Této technice napodobování čísel se říká spoofing¹⁹. Jako příklad bude sloužit případ ženy z Prahy, která po vishingovém telefonátu přišla o téměř všechny úspory.

Žena zvedla příchozí hovor, který se na displeji jevil jako hovor z banky. Na druhé straně se představil „bankéř“, který oznámil, že účet klientky byl napaden. Sdělil jí také obavu, že se mohlo jednat o únik dat způsobený nějakým jiným bankéřem, který pravděpodobně prodal její data třetí straně. Podvodník poté ženě řekl, že tuto skutečnost oznámí policii a ta ji bude později kontaktovat. Policie ji opravdu po několika minutách kontaktovala, ovšem to vše bylo součástí podvodu. „Policista“ si s obětí plánuje schůzku, aby přidal celé historce důvěryhodnost, ovšem k té nikdy nedojde. Místo toho se opět ozve „banka“ s tím, že oběti sdělí řešení celé této situace, aby nepřišla o peníze. První krok, který falešný bankéř

¹⁸ *What is vishing?* Online. Terranova security. 2022. Dostupné z: <https://terrانovasecurity.com/what-is-vishing/>. [cit. 2024-03-06].

¹⁹ *Vishing a spoofing*. Online. Policie České republiky. 2021. Dostupné z: <https://www.policie.cz/clanek/vishing-a-spoofing.aspx#:~:text=Fiktivn%C3%AD%20bankovn%C3%AD%20%C3%BA%C5%99edn%C3%ADk%20vystra%C5%A1%C3%AD%20r%C5%AFzn%C3%BDmi,pouze%20o%20do%C4%8Dasn%C3%A9%20bezpe%C4%8Dnostn%C3%AD%20opat%C5%99en%C3%AD.> [cit. 2024-03-06].

sdělí, je požádání o úvěr, přičemž oběť emočně a psychicky manipuluje. Dalším krokem je navýšení limitů výběrů a výběr všech peněz z účtu. Po výběru podvodník oběť navede, aby uložila vybranou částku na „bezpečný“ účet. Tímto ji donutí nakoupit kryptoměnu Bitcoin, kterou si od oběti vyzvedne a následně dokoná celý podvod.

Ale tím to končit nemusí. Pachatel může dojít tak daleko, že bude poškozeného vydírat. Slibuje vrácení kradeného peněžního obnosu, pokud mu budou zaslány intimní fotografie. To je samozřejmě lež a v případě, že by intimní fotografie opravdu obdržel, tak by je využil k další vlně vydírání a nátlaku na oběť²⁰.

2.6 Investiční podvody

V digitální době, která nás obklopuje, dochází k revoluci nejen v komunikaci a technologiích, ale i v oblasti investic. Digitalizace otevřela nové možnosti pro jednodušší a přístupnější investování. Tato změna je hlavně spojena s online platformami, které nám pomáhají jednoduše a efektivně spravovat finanční instrumenty.

Ovšem s tím také přichází nová rizika. V poslední době se častěji dostávají na povrch informace o investičních podvodech. Tyto podvody mohou mít různé formy a často slibují vysoké výnosy nebo zisky s minimálním rizikem. Pachatelé vytvoří a umístí na web reklamu, která láká na zisk z investic. Reklamy mohou vypadat důvěryhodně, protože zpravidla využívají tvář známé osobnosti nebo společnosti. Poté co se oběť zaregistruje, je ihned kontaktována pachatelem, který se vydává za ochotného investičního poradce²¹. Ten poté navede oběť ke stažení software se vzdáleným přístupem k počítači, konkrétně např. TeamViewer, AnyDesk nebo Supremo. Tím pachatel dostane přístup k osobním informacím, a hlavně internetovému bankovníctví, díky čemuž jednotlivce připraví o peníze.

Mezi takové patří i případ staršího muže z Velkých Losin, který obdržel telefonát „burzovního makléře“ na podzim roku 2023. Podvodný makléř seniora přesvědčil k instalaci aplikaci pro vzdálený přístup, aby mu pomohl s investováním na burze.

²⁰ *Podvodníci, kteří se vydávají za Policii*. Online. YouTube. Dostupné z: <https://www.youtube.com/watch?v=rB0x09uAyyE>. [cit. 2024-03-07].

²¹ *Podvod s investicemi*. Online. Policie České republiky. 2023. Dostupné z: <https://www.policie.cz/clanek/podvod-s-investicemi.aspx>. [cit. 2024-03-07].

Poškozený nezhodil možná rizika a pachateli poslal celkovou částku okolo 107 000 Kč. Podvodníkovy úmysly starší muž odhalil až ve chvíli, kdy požadoval zaslání vydělané částky zpět na svůj účet. Setkal se s neochotou a argumenty, že musí investovat víc, aby přeci vydělal. Seniora napadlo, že by se mohlo jednat o podvod a kontaktoval policii, která jeho domněnku potvrdila a sdělila, že zaslané peníze už pravděpodobně neuvidí²².

Můžeme tvrdit, že v oblasti sociálního inženýrství byly poslední 2 roky poměrně revoluční. V roce 2023 zaplavily český internet falešné reklamy s investicemi. Podvodníci využili tváří známých politiků, podnikatelů, či dokonce prezidenta České republiky. Petr Pavel v jednom z těchto videí upozorňuje na vysoké zhodnocení investované částky a oznamuje spuštění nové platformy, která umožňuje vydělávat peníze kdykoliv a kdekoliv. Stejně tak kandidát na prezidenta, Andrej Babiš, láká na investice a slibuje týdenní pasivní příjem o astronomických částkách. Obě politické figury byly zneužity podvodníky, jelikož vzbuzují v lidech důvěru a začátkem roku 2023 byly na televizních obrazovkách téměř každý den. Odborníci na kybernetickou bezpečnost se shodují, že se jedná o nejpovedenější videa tohoto typu a jejich kvalita se bude s vývojem umělé inteligence nadále zvyšovat²³.

2.7 Skimming

Skimming je protiprávní jednání, které zahrnuje neoprávněné získání citlivých informací z magnetického proužku platební karty. Dochází k tomu tak, že pachatelé nainstalují zařízení do bankomatu nebo na jiné čtecí zařízení. Když je karta vložena do bankomatu, data z magnetického proužku se zkopírují na předem připravený nosič dat²⁴.

²² *Investice ho stála 107 000 Kč.* Online. Policie České republiky. 2023. Dostupné z: <https://www.policie.cz/clanek/investice-ho-stala-107-000-kc.aspx>. [cit. 2024-03-06].

²³ *Když Pavel či Babiš radí s investicemi. Podvodníci na internetu se zlepšují.* Online. IDNES. 2024. Dostupné z: https://www.idnes.cz/zpravy/domaci/umela-inteligence-deep-fake-video-pavel-babis.A240209_192239_domaci_pukk. [cit. 2024-03-07].

²⁴ *Skimming.* Online. Policie České republiky. 2014. Dostupné z: <https://www.policie.cz/clanek/ncoz-skimming.aspx>. [cit. 2024-03-07].

2.8 Libanonská smyčka a zadržení hotovosti

Zachycení platební karty, též nazýváno libanonská smyčka, je podvodné jednání, které spočívá v zásahu do bankomatu. Pachatel vloží do štěrbinu na kartu technické zařízení, které zadrží platební kartu oběti. Pachatel se může nacházet poblíž a nabídne oběti pomoc. Vyzve ji ke znovuzadání kódu PIN, který si zapamatuje a po odchodu oběti si platební kartu z bankomatu vezme.

Zadržení hotovosti využívá podobnou taktiku jako libanonská smyčka – pachatel neoprávněně instaluje zařízení do bankomatu. V tomto případě se jedná o instalaci lišty, která vypadá jako součást bankomatu, ale ve skutečnosti má za úkol blokovat vydání hotovosti a budit dojem, že výběr nebyl úspěšný²⁵.

2.9 Praní špinavých peněz

Praní špinavých peněz představuje proces, jehož cílem je zamaskovat nelegálně získané finanční prostředky tak, aby bylo těžké sledovat jejich původ a spojit je s původním trestným činem. Peníze z kriminální činnosti jsou považovány za nečisté, a proces praní peněz slouží k tomu, aby vypadaly jako legálně nabyté.

Praní peněz je primárně spojeno s organizovaným zločinem. Kriminální organizace využívají tento proces, aby efektivně využily své nelegálně získané finanční prostředky. Potřebují uložit tyto peníze do finančních institucí, ale to mohou pouze, pokud bude původ peněz vypadat legitimně²⁶.

Proces praní zpravidla zahrnuje tři kroky²⁷:

- **Umístění** – V této fázi zločinci vkládají peníze do finančního systému.
- **Vrstvení** – Zakrývá pravý původ peněz skrze řetězec transakcí.
- **Integrace** – Vyprané peníze mohou být vyzvednuty z účtu a užívány jako legálně nabyté.

²⁵ Platím kartou. Online. PCI Standard. 2023. Dostupné

z: <https://www.pcistandard.cz/pcidss/drzitel/#:~:text=Podvodn%C3%ADk%20vlo%C5%BE%C3%AD%20do%20%C5%A1t%C4%9Brbiny%20%C4%8Dte%C4%8Dky,si%20podvodn%C3%ADk%20zapamatuje%20nebo%20zaznamen%C3%A1.> [cit. 2024-03-07].

²⁶ What Is Money Laundering? Online. Investopedia. 2024. Dostupné

z: <https://www.investopedia.com/terms/m/moneylaundering.asp>. [cit. 2024-03-07].

²⁷ Co to je praní peněz. Online. Česká národní banka. 2020. Dostupné

z: https://www.cnb.cz/cs/o_cnb/cnbblog/Co-to-je-prani-penez. [cit. 2024-03-07].

2.10 Podvody spojené s kryptoměnou

Kryptoměny se v posledních několika letech stávají velmi oblíbenou položkou pro investice, nicméně v České republice se netěší takové popularitě, jako v jiných zemích. Právě proto jsou tyto druhy podvodu méně obvyklé, ovšem neméně nebezpečné.

Nejčastější podvody zahrnují "Investiční manažery", kteří slibují rychlé a několikanásobné zisky po investici. Pachatelé se také mohou vydávat za známé osobnosti nebo společnosti a nabízejí výdělků v podobě kryptoměn nebo tokenů.

Trestná činnost s kryptoměnami je ovšem rozsáhlejší, než se na první pohled může zdát. Díky anonymitě, kterou kryptoměny disponují, se zpravidla využívají na černém trhu a dark webu. Může se jednat o falešné e-shopy, trh s nelegálním obsahem nebo blackmailing.

2.11 Love fraud

Tento typ podvodu obvykle začíná vytvořením falešné identity v online prostředí a následném získání důvěry nebo citového pouta oběti. Po navázání vztahu může podvodník požadovat finanční prostředky nebo dary od své oběti. Na love fraud lze narazit téměř na jakékoliv platformě, ovšem nejčastěji na sociálních sítích nebo seznamovacích platformách. Účelem je získat si důvěru oběti a díky manipulaci ji přimět k finančním transferům. Zpravidla se jedná o dlouhodobý kontakt, ovšem tento druh podvodu může mít pro oběť obzvlášť závažné následky. Mimo finanční ztráty může utrpět emoční trauma a pocit zrad.

2.12 Podvod s nigerijským princem

Tento podvod obvykle začíná e-mailem nebo dopisem, ve kterém se tvrdí, že odesílatel je vlivná osoba, která má velké množství peněz uložených v zemi a potřebuje pomoc s jejich přesunem do zahraničí. Podvodníci obvykle slibují, že pokud oběť poskytne své bankovní údaje nebo předem zaplatí poplatky, získá podíl na těchto penězích. Tento podvod je často spojen s nejrůznějšími scénáři a příběhy, ale vždy končí požadavkem na poskytnutí peněz či osobních údajů oběti. Podvod s nigerijským princem je považován za typický příklad "předplaceného

podvodu", kdy podvodníci slibují velké finanční odměny nebo výhody, ale skutečným cílem je získat peníze nebo citlivé informace od oběti.

V této době jsou podobné podvody na ústupu, ale nezmizely úplně, spíše změnilly kabátek. Na jeden z podvodných inzerátů odpověděla žena z Vysočiny. Měla zaplatit určitý vklad a poté nainstalovat aplikaci, aby získala značný výdělek z kryptoměn. Podvodník tak získal přístup k osobním údajům a finančním prostředkům, ze kterých odčerpал desetitisíce českých korun²⁸.

²⁸ *Jsem nigerijský princ: Podvodníci s kryptoměnou útočí stále časteji*. Online. Deník.cz. 2021. Dostupné z: <https://www.denik.cz/krimi/jsem-nigerijsky-princ-podvodnici-s-kryptomenou-utoci-i-na-vysocine-20210905.html>. [cit. 2024-03-06].

3 Ochrana platebního styku

Vzhledem k množství trestné činnosti spojené s platebním stykem je klíčovým prvkem bezpečnost. V rámci této bezpečnosti je nezbytné zajistit opatření, právní ochranu spotřebitelů nebo institucí a prevenci potenciálních rizik. Banky a platební instituce v České republice spolupracují s regulátory a dohlížejíci orgány, jako je Česká Národní Banka, aby zajistily, že platební služby jsou poskytovány v souladu s nejvyššími standardy bezpečnosti.

S příchodem moderních platebních metod, jako jsou mobilní platby a digitální peněženky, se ochrana platebního styku stává ještě komplexnější. Česká národní banka aktivně sleduje nové technologické trendy a aktualizuje předpisy tak, aby zajistila bezpečnost v platebním prostředí.

V této kapitole se podíváme, jak Česká republika reaguje na ohrožení stability finančního systému. Právní předpisy, které tvoří samotný finanční systém, opatření, zabývající se ochranou měny nebo bezhotovostních plateb, ale také institucionální strukturu.

3.1 Právní úprava

V České republice je platební styk regulován komplexním souborem právních předpisů, které mají za cíl zajišťovat bezpečnost, spolehlivost a efektivnost platebních transakcí. Mezi klíčové součásti této regulace patří zákony, nařízení a směrnice, které jsou v souladu s evropskými standardy a mezinárodními dohodami. Hlavním právním dokumentem upravujícím platební styk v České republice je zejména zákon č. 370/2017 Sb., o platebním styku, ve znění změn provedených zákonem č. 129/2022 Sb. Tento pramen stanovuje podmínky pro provozování platebních institucí, včetně bank a jiných finančních subjektů, které poskytují platební služby. Tyto podmínky zahrnují licenční požadavky, povinnosti týkající se transparentnosti a informovanosti spotřebitelů a pravidla pro ochranu finančních prostředků.

Dále stanovuje bezpečnostní požadavky pro poskytovatele platebních služeb s cílem chránit spotřebitele před podvody a zneužití platebních údajů. To zahrnuje například požadavky na dvoufaktorové ověření pro online platební transakce a

povinnost informovat spotřebitele o rizicích spojených s platebními službami. Spotřebitelé mají právo na jasné a srozumitelné informace o poplatcích, podmínkách a rizicích spojených s používáním platebních služeb.

Česká právní úprava platebního styku a jeho bezpečnosti je propojena s právními prameny Evropské unie. Evropská unie vytváří základní rámec a standardy pro fungování platebních systémů a elektronických plateb, které jsou poté implementovány do vnitrostátní legislativy členských států, včetně České republiky. Tato harmonizace právních předpisů umožňuje snazší interoperabilitu platebních systémů v rámci jednotného trhu EU, zvyšuje bezpečnost elektronických plateb a posiluje ochranu spotřebitelů.

Jedním z příkladů evropských právních předpisů, které ovlivňují českou právní úpravu platebního styku, je Směrnice o platebních službách (PSD2). Tato směrnice, přijatá Evropskou unií v roce 2015 a následně novelizovaná v roce 2018, má za cíl modernizovat a zvýšit bezpečnost platebních systémů v EU. PSD2 zavádí požadavky na dvoufaktorovou autentizaci při elektronických platebních transakcích, což pomáhá snižovat riziko podvodů a zajišťuje vyšší úroveň bezpečnosti pro spotřebitele²⁹.

Dalším důležitým zákonem, který přímo navazuje na Evropskou legislativu, je zákon č. 136/2011 Sb., také známý jako Zákon o oběhu bankovek a mincí. Tento právní předpis stanovuje pravidla pro vydávání, oběh bankovek a mincí, dozor nad výrobou a distribucí, způsoby znehodnocení poškozených bankovek a mincí, a také postupy pro likvidaci neplatných platebních prostředků. Kromě toho tento zákon stanovuje pravidla pro vyplácení bankovek a mincí a upravuje trestní odpovědnost za padělání a poškozování platebních prostředků. Evropská unie vydává směrnice a nařízení týkající se měnové politiky a ochrany eura, které mají za cíl zajistit jednotnost a stabilitu měnového systému v rámci EU. Zákon o oběhu bankovek a mincí v České republice je tedy koncipován tak, aby respektoval a implementoval tyto evropské právní předpisy.

²⁹ *The revised Payment Services Directive (PSD2) and the transition to stronger payments security.* Online. EUROPEAN CENTRAL BANK. 2018. Dostupné z: https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html. [cit. 2024-03-07].

Zakotvení hotovostních plateb do ústavy České republiky

V současné době je diskutováno případné ústavní zakotvení práva na placení v hotovosti v České republice. Opoziční poslanci z hnutí SPD předložili návrh na doplnění ústavní listiny práv a svobod o právo na placení hotovostí, který však narazil na odpor koaličního kabinetu Petra Fialy³⁰.

Návrh SPD zdůvodňuje ochranou soukromí obyvatel a zdůrazňuje důležitost hotovostních plateb jako nástroje zajišťujícího svobodu a soukromí občanů. Tento návrh reaguje na obavy z postupného omezení a zrušení možnosti hotovostních plateb a varuje před rizikem zneužití informací shromažďovaných v souvislosti s bezhotovostními platbami.

Naopak, vláda argumentuje, že hotovostní platby již dostatečně upravuje platný právní řád a nevidí důvod pro jejich zákonem stanovené povinné přijímání. Podle ní by taková úprava zasáhla do autonomie vůle a zásady smluvní volnosti, kdy je možné se domluvit na způsobu platby. Zároveň poukazuje na existenci trestních sankcí pro odmítání tuzemských peněz bez zákonného důvodu.

Návrh SPD by se navíc nevztahoval pouze na české peníze, ale i na cizí měnu, což je další argument, který vláda používá proti tomuto návrhu. Podle ní není takové vymezení dostatečné a současný právní řád již obsahuje dostatečná opatření k ochraně bezpečnosti a veřejného pořádku.

Diskuze o ústavním zakotvení práva na hotovostní platby ukazuje na komplexnost problematiky a rozdílné pohledy na roli a význam hotovostních plateb v moderní společnosti. Zatímco někteří zdůrazňují důležitost hotovosti pro ochranu soukromí a svobody občanů, jiní vidí v bezhotovostních platbách výhody rychlosti, pohodlí a bezpečnosti.

AML

Anti Money Laundering (dále jen AML) je soubor právních a regulačních opatření navržených k zabránění použití finančního systému k legalizaci příjmů z trestné činnosti. Jeho cílem je detekovat a zabránit praní špinavých peněz, tj. proces, při

³⁰ *Právo na placení hotovostí v Ústavě? Vláda návrh označila za nadbytečný.* Online. Seznam zpráv. 2023. Dostupné z: <https://www.seznamzpravy.cz/clanek/ekonomika-pravo-na-placeni-hotovosti-v-ustave-vlada-navrh-oznacila-za-nadbytecny-234676>. [cit. 2024-03-06].

kterém jsou finanční prostředky získané nezákonným způsobem proměněny na zákonné. Mezi nejdůležitější normy v této oblasti patří zákon 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, který byl změněn zákony č. 368/2016 Sb a 527/2020 Sb.

Na základě těchto právních norem jsou finanční instituce povinny shromažďovat informace o svých klientech a provádět důkladné ověření jejich identity, což se dělá pomocí platných identifikačních dokumentů, jako jsou občanské průkazy, pasy nebo jiné oficiální doklady. Tento proces je znám jako KYC (Know Your Client – Poznej Svého Klienta) a slouží k posouzení rizika daného klienta. Dalším důležitým prvkem je monitorování finančních transakcí a hledání neobvyklých vzorů, které by mohly naznačovat praní špinavých peněz nebo financování terorismu. Implementace AML opatření v České republice je kontrolována Českou národní bankou a Finančním analytickým úřadem, které mají za úkol zajišťovat dodržování právních předpisů v této oblasti a provádět dozorovou činnost nad finančními institucemi a dalšími subjekty.

3.2 Česká národní banka

Česká národní banka (ČNB) zastává důležitou úlohu v oblasti platebního styku v rámci České republiky. Jako centrální banka státu má na starosti dohled nad finančním trhem a je pověřena zajištěním stability a bezpečnosti platebního systému, což je obzvláště důležité v době rostoucích hrozeb spojených s kybernetickou kriminalitou a podvody.

Úloha ČNB je zakořeněna v právním rámci České republiky, který ji ustanovuje jako nezávislý orgán s pověřením chránit a udržovat stabilitu finančního sektoru. Tato nezávislost je zásadní pro efektivní vykonávání měnové politiky a ochranu platebního styku před různými formami hrozeb.

V souladu se svými pravomocemi vykonává ČNB dohled nad bankami, platebními institucemi a dalšími subjekty podílejícími se na platebním styku. Jedním z hlavních úkolů je poskytování ochrany a zajištění bezpečnosti finančních transakcí v rámci platebního systému. To zahrnuje monitorování a regulaci platebních metod, implementaci bezpečnostních standardů a přijímání opatření k prevenci podvodů a kybernetických útoků.

Jako součást své role vyvíjí ČNB strategie a politiky zaměřené na zlepšení bezpečnosti platebních operací. To může zahrnovat spolupráci se zainteresovanými stranami, jako jsou banky a bezpečnostní odborníci, aby se identifikovaly potenciální hrozby a navrhla účinná opatření k jejich řešení³¹. V neposlední řadě je ČNB klíčovým hráčem v rámci mezinárodní spolupráce v oblasti bezpečnosti platebního styku. Jako člen Evropského systému centrálních bank aktivně spolupracuje s dalšími centrálními bankami a orgány dohledu v rámci EU na výměně informací a osvědčených postupů v boji proti hrozbám v oblasti platebních systémů. Její úsilí směřuje k ochraně spotřebitelů, prevenci podvodů a posilování důvěry v platební systém prostřednictvím implementace bezpečnostních opatření a spolupráce s ostatními subjekty v oblasti finančních služeb.

³¹ *Pravomoci bankovního dohledu*. Online. Česká národní banka. 2024. Dostupné z: <https://www.cnb.cz/cs/dohled-financni-trh/vykon-dohledu/postaveni-dohledu/dohled-nad-uverovymi-institucemi/pravomoci-bankovniho-dohledu/>. [cit. 2024-03-07].

3.3 Finanční analytický úřad

Významnou roli v oblasti AML má Finanční analytický úřad (FAÚ). Jedná se o správní orgán, který vznikl jako finanční zpravodajská jednotka v roce 2017. FAÚ je pověřen prováděním úkolů vyplývajících ze zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, a zákona č. 69/2006 Sb., o provádění mezinárodních sankcí. Jedním z hlavních úkolů FAÚ je sběr a analýza informací o podezřelých finančních operacích. Tyto informace jsou klíčové pro identifikaci a vyšetřování potenciálně nelegálních aktivit v platebním styku. Důležitou součástí činnosti FAÚ je také zpracování návrhů na rozvoj a zdokonalení opatření proti praní peněz a financování terorismu v souladu s národními a mezinárodními právními předpisy.

FAÚ úzce spolupracuje s dalšími institucemi, včetně zpravodajských služeb, Policií České republiky a ministerstev, aby zajistil efektivní výměnu informací a koordinaci opatření v oblasti bezpečnosti platebního styku. Na mezinárodní úrovni FAÚ navazuje spolupráci s obdobnými institucemi v členských státech NATO a Evropské unie, což umožňuje efektivní řešení přeshraničních zločineckých aktivit.

Oprávnění FAÚ jsou jasně definována v právních předpisech, což zahrnuje možnost provádět vyšetřování a vydávat rozhodnutí ve správním řízení souvisejícím s bojem proti praní peněz a financování terorismu. Tato oprávnění poskytují FAÚ široký rámec pro svou činnost a umožňují mu účinně reagovat na aktuální hrozby v oblasti bezpečnosti platebního styku³².

3.4 Finanční arbitr

Finanční arbitr představuje státem zřízený orgán pro mimosoudní řešení spotřebitelských sporů na finančním trhu. Povinnosti finančního arbitra vyplývají ze zákona 229/2002 Sb., o finančním arbitrovi, ve znění pozdějších předpisů. Jeho

³² *Legislativa a metodika*. Online. Finanční analytický úřad. 2020. Dostupné z: [https://fau.gov.cz/legislativa-a-metodika-459#:~:text=Z%C3%A1kladn%C3%ADm%20pr%C3%A1vn%C3%ADm%20p%C5%99edpisem%20obsahuj%C3%ADc%C3%ADm%20pravidla,tak%C3%A9%20%E2%80%9EAML%20z%C3%A1kon%E2%80%9C\).](https://fau.gov.cz/legislativa-a-metodika-459#:~:text=Z%C3%A1kladn%C3%ADm%20pr%C3%A1vn%C3%ADm%20p%C5%99edpisem%20obsahuj%C3%ADc%C3%ADm%20pravidla,tak%C3%A9%20%E2%80%9EAML%20z%C3%A1kon%E2%80%9C).) [cit. 2024-03-06].

úkolem je řešit spory mezi spotřebiteli a finančními institucemi v oblastech, jako jsou platební služby, úvěry, pojištění a další. Finanční arbitr rozhoduje pouze na základě návrhu spotřebitele a usiluje zejména o smírné vyřešení sporu. Nicméně existují situace, kdy finanční arbitr nemůže rozhodnout, například pokud spor nenáleží do jeho působnosti, již byl řešen soudem nebo jiným arbitrem, nebo pokud návrh neobsahuje veškeré potřebné náležitosti.

Řízení před finančním arbitrem je bezplatné a strany se nemusí právně zastupovat. Finanční arbitr rozhoduje na základě skutečností zjištěných v souladu se zákonem a poskytuje oběma stranám možnost vyjádření a předkládání důkazů. Jeho rozhodnutí je přezkoumatelné soudem, který může rozhodnutí potvrdit, změnit nebo zrušit. Náklady řízení si nesou strany samy, a finanční arbitr nemůže přiznat náklady na právní zastoupení. Proti rozhodnutí finančního arbitra lze podat odůvodněné námitky a proti pravomocnému rozhodnutí se lze odvolat k soudu. Pro využití služeb finančního arbitra je třeba podat písemný návrh obsahující určité náležitosti, včetně označení účastníků řízení, důkazů a domáhání se určitého opatření. Řízení může být zahájeno pouze na návrh spotřebitele³³.

³³ *Pravomoc a působnost*. Online. Kancelář finančního arbitra. 2019. Dostupné z: <https://finarbitr.cz/cs/reseni-sporu/pusobnost-financniho-arbitra.html>. [cit. 2024-03-06].

3.5 Ochrana bankovek a mincí

V minulé kapitole jsem zmínil, že pozměňování a padělání platebních prostředků je značným problémem v jakékoli společnosti. Na českých bankovkách jsou implementovány různé ochranné prvky, které mají zabránit jejich padělání a zajišťují bezpečnost platebních prostředků.

Ochranné prvky bankovek:

1. Bankovní papír

Používá se pro tisk bankovek. Už samotný papír slouží jako ochranný prvek, kvůli jeho specifické struktuře. Má speciální barvu, pružnost a pevnost, aby bylo složitější jej napodobit.

2. Vodoznak

Vodoznak je viditelný při pohledu na bankovku proti světlu. Zpravidla obsahuje nominální hodnotu a tvář osobnosti, která je vyobrazená na čelní straně bankovky. V případě 2000 Kč se jedná o tvář slavné české operní pěvkyně Emy Destinové.

3. Okénkový proužek s mikrotextem

Okénkový proužek můžeme po částech vidět z obou stran bankovky. Je tvořen kovově lesklou hmotou zapuštěnou do papíru o šířce 3 mm. Ovšem při pohledu proti světlu lze odhalit souvislý pruh, který má tmavou barvu a obsahuje mikrotext.

4. Barevná vlákna

Jedná se o vlákna oranžové barvy, které lze spatřit pouhým okem v bílých částech bankovky. Jejich délka je 6 mm a tvoří další vrstvu ochrany.

5. Soutisková značka

Část značky je viditelná z rubu a část z líce bankovky. Prosvícením se soutisková značka zcelí a tvoří ji písmena "ČR".

6. Skrytý obrazec

Skrytý obrazec je vytvořen pomocí speciálních tiskových technik, které umožňují jej spatřit pouze při určitém osvětlení nebo úhlu pohledu. Nachází se na lící straně a tvoří ho číslo označující nominální hodnotu. Při sledování z různých úhlů lze spatřit jeho proměnlivou barvu, která je buď tmavá nebo světlá.

7. Proměnlivá barva

Proměnlivá barva některých prvků bankovky je založená na optickém efektu. V závislosti na dopadu světla se bude barva měnit, například u bankovky s nominální hodnotou 2000 Kč se jedná o struny lyry. Ty se mění ze zlaté na zelenou.

8. Iridiscentní pruh

Jedná se o duhově lesklý pruh, který se nachází na pravé straně bankovky z lící strany.

9. Mikrotext

Mikrotext je dalším důležitým bezpečnostním prvkem na českých bankovkách. Jedná se o drobný text, který je tisknutý na bankovce a je téměř nečitelný pouhým okem. Pro jeho viditelnost je obvykle zapotřebí použití lupy. Tvořen je tiskem z plochy a hloubky³⁴.

Ochranné prvky mincí:

U mincí jsou ochrannými prvky jak specifický design, tak technické parametry. Zpravidla jsou tvořeny ocelí a galvanicky pokoveny niklem, mědí nebo zinkem. Hrany mince mohou být hladké, vroubkované a hranaté. Na lící straně je vyobrazen český lev, na straně rubové jsou symboly charakteristické pro Českou republiku (ČNB).

³⁴ *Ochranné prvky 2000 Kč*. Online. Česká národní banka. 2010. Dostupné z: <https://www.cnb.cz/cs/bankovky-a-mince/bankovky/ochranne-prvky-2000-kc/>. [cit. 2024-03-07].

3.6 Ochrana platebních karet

Platební karty jsou moderní nástroje bezhotovostního platebního styku, které umožňují držitelům provádět různé finanční transakce, a to jak v kamenných obchodech, tak online. Uživatelé u sebe nemusí nosit velké finanční částky, protože karty jsou zpravidla napojené na běžné nebo úvěrové účty u bankovních institucí. Tento nástroj také umožňuje zrychlení prodejního procesu, jelikož kartu stačí pouze přiložit k platebnímu terminálu. Kdykoli ovšem manipulujeme s kartou, vystavujeme se tím riziku, jelikož hrozby nečíhají pouze na internetu. V této podkapitole se podíváme na bezpečnostní prvky platebních karet a jak předcházet nebezpečí zneužití platební karty.

Mezi nejčastější bezpečnostní prvky karty patří:

Datový čip – Obsahuje identifikační údaje karty

Číslo karty – Jedná se o šestnáctimístné číslo pro platby na internetu.

Logo karetní asociace (Visa, MasterCard...)

Logo a název banky (KB, ČSOB...)

Platnost karty – Jedná se o číslo ve tvaru měsíc/rok, které je nutné pro úspěšnou platbu online (např 06/24)

Jméno a příjmení držitele

Kontaktní údaje – V případě problému lze kontaktovat banku, která kartu vydala.

Magnetický proužek – Proužek černé barvy, na kterém jsou uloženy údaje o kartě.

Podpisový proužek – Je nezbytné kartu po převzetí podepsat. Obchodník může nepodepsanou kartu odmítnout.

CVC/CVV kód – Další vrstva ochrany pro platby na internetu³⁵.

³⁵ *Jak bezpečně využívat platební karty.* Online. ČSOB. 2015. Dostupné z: <https://www.csob.cz/branteseroumem/zasady-bezpecneho-chovani/jak-bezpecne-vyuzivat-platebni-karty>. [cit. 2024-03-07].

Prevence ohrožení platební karty

Bankovní instituce na svých internetových stránkách zpravidla radí, jak přistoupit k ochraně platebních karet. Základem jsou správně nastavené limity pro výběr nebo platby, zasílání oznámení o transakcích a pravidelná kontrola výpisů. Kartu používejte pouze u důvěryhodných obchodníků, chraňte svůj PIN a pokud je na výběrovém bankomatu cokoli podezřelého, transakci zrušte a kontaktujte klientskou linku dané banky. Při ztrátě nebo odcizení karty jednejte rychle a pomocí telefonátu s klientskou linkou ji co nejdříve zablokujte.

Dvoufázová autentizace

Jedná se o formu zabezpečení online plateb na chytrých telefonech. Pokud uživatel platí kartou na e-shopu, může být vyzván k potvrzení heslem v aplikaci, která je pro dvoufázové ověření určena. Každá banka má svou aplikaci (KB klíč, Smart klíč, George klíč...), která funguje jako „silné ověření klienta“. Upozornění v aplikaci stačí potvrdit zadáním hesla, otiskem prstu nebo scanem obličeje.

3.7 Ochrana internetového bankovníctví

Bezpečnost internetového bankovníctví je jednou z priorit bankovních institucí v dnešní digitální době, kdy se stále více finančních transakcí přesouvá do online prostředí. Hlavním cílem je chránit klienty před kybernetickými hrozbami a zajistit bezpečnost jejich finančních prostředků. Uživatelské jméno a heslo jsou tradičním způsobem autentizace, který je stále široce používán. Jsou jednoduché na použití, avšak náchylné k útokům typu prolomení hesla nebo phishingu. Podpisový certifikát, uložený na čipu nebo v kartě, poskytuje další vrstvu ochrany při provádění finančních transakcí online. Certifikát je unikátně spojen s uživatelem a zajišťuje nedotknutelnost při podepisování transakcí. Nevýhodou může být potenciální riziko ztráty či odcizení tohoto zařízení. Podobnou funkci jako podpisový certifikát plní i autentizační SMS nebo biometrika. V případě potvrzování skrz zprávy je klientovi zaslána SMS s jednorázovým kódem, který musí zadat pro ověření identity. Výhodou tohoto systému je jeho jednoduchost a rychlost, ovšem je zde riziko v případě kopírování karet SIM nebo přístup útočníka k telefonnímu číslu klienta. Na druhou stranu biometrické ověřování poskytuje

vysokou úroveň bezpečnosti a pohodlí pro uživatele. Biometrická data jsou unikátní pro každého jednotlivce, což ztěžuje jejich padělání. Mezi nejčastější biometrické metody identifikace patří otisk prstu nebo rozpoznání obličeje³⁶.

Dalším klíčovým prvkem bezpečnosti internetového bankovníctví je šifrování dat, které zpravidla funguje na principu koncového šifrování. Při tomto procesu jsou veškeré informace přenášeny mezi klientem a bankou převedeny do nečitelného formátu, který je chráněn před odposlechem a manipulací třetími stranami. Tento proces zajišťuje bezpečnost citlivých údajů, jako jsou hesla, čísla kreditních karet a finanční transakce³⁷.

Celkově je důležité kombinovat různé bezpečnostní prvky pro dosažení co nejvyšší úrovně bezpečnosti internetového bankovníctví. Žádný z těchto prvků není dokonalý, ale společné použití více vrstev ochrany může výrazně snížit riziko úspěšného kybernetického útoku.

³⁶ *Víte, jak ochránit své peníze na internetu?* Online. Moneta. 2019. Dostupné z: <https://www.moneta.cz/caste-dotazy/odpoved/vite-jak-ochranit-sve-penize-na-internetu>. [cit. 2024-03-07].

³⁷ *Šifrování dat.* Online. ESET. 2019. Dostupné z: <https://www.eset.com/cz/firmy/firemni-reseni/sifrovani/>. [cit. 2024-03-07].

4 Praktická část

Bezpečnost platebního styku je téma, které se týká jak individuálně každého z nás, tak společnosti jako celku. Proto jsem si dal za cíl vypracovat praktickou část, která bude poslední kapitolou v této bakalářské práci. Jedním z cílů je zjistit jakému druhu platebního styku občané důvěřují více. Dalším cílem je prozkoumat povědomí veřejnosti ohledně znalosti rizik a (ne)bezpečí v platebním prostředí. Pro získání dat v této kapitole jsem zvolil výzkumnou metodu dotazníkového šetření. Dotazník je ve formě kvantitativního šetření a lze ho nalézt v příloze č. 2 na konci práce.

Výzkumné předpoklady:

1. Naprosté minimum respondentů nedůvěřuje bezhotovostní platbě.
2. Většina respondentů preferuje bezhotovostní platby.
3. Většina respondentů zná ochranné prvky u bankovek a platebních karet.
4. Osoby nad 40 let preferují spíše hotovostní platbu než bezhotovostní.
5. Nejčastějším podvodem, se kterým se respondenti setkali je phishing.

Výběr respondentů

K tvorbě dotazníku jsem využil nástroje internetové stránky www.survio.com, přímý odkaz jsem následně sdílel na svých sociálních sítích, šířil přes e-mail a soukromé zprávy, abych dostal co největší vzorek respondentů. Šetření obsahovalo celkem 17 otázek, z nichž 14 bylo zaměřeno na platební styk a jeho bezpečnost. Poslední 3 otázky se týkaly demografického hlediska. Nakonec anketu vyplnilo celkem 107 osob.

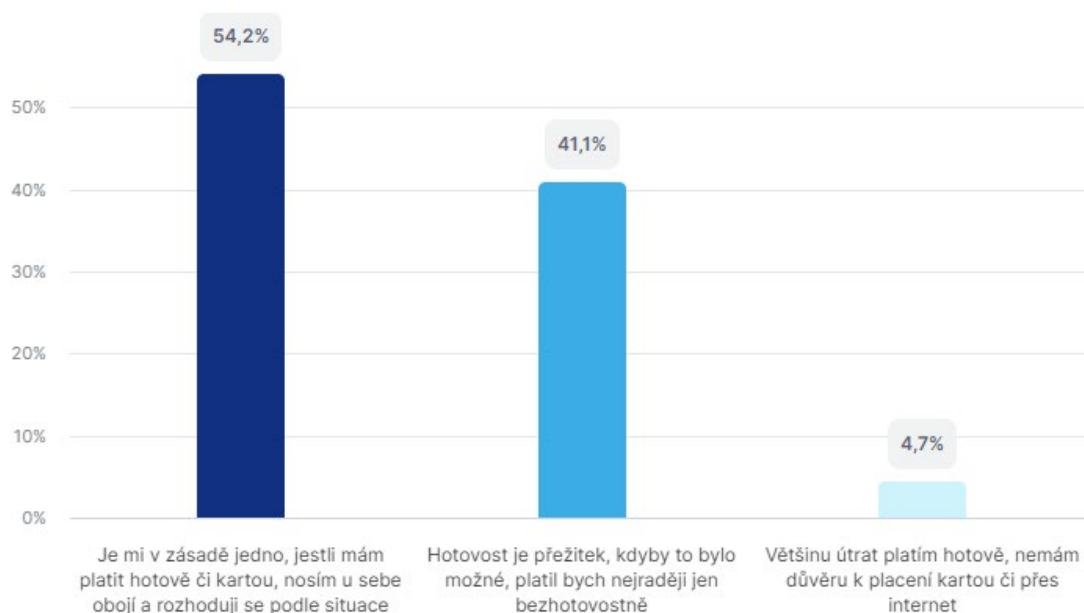
4.1 Výsledky dotazníkového šetření

Výsledky otázek jsem zpracoval do grafů a jsou znázorněny v relativních číslech, abych mohl jednoduše porovnat své výzkumné předpoklady se získanými informacemi.

Z průzkumu jsem zjistil, že většina respondentů preferuje bezhotovostní platby, v drtivé většině se jedná o platební karty a zařízení podporující technologii NFC. Může za to hlavně snadný přístup k financím a zrychlení procesu převodu peněz mezi dvěma subjekty.

Hotovost je stále aktuální a lidé ji využívají hlavně při placení menších částek. Naopak čím větší obnos je potřeba zaplatit, tím roste i pravděpodobnost, že se obrátí na bezhotovostní platbu.

Graf č. 1 - Co z následujícího nejlépe charakterizuje vaše zvyklosti při placení za nákupy?

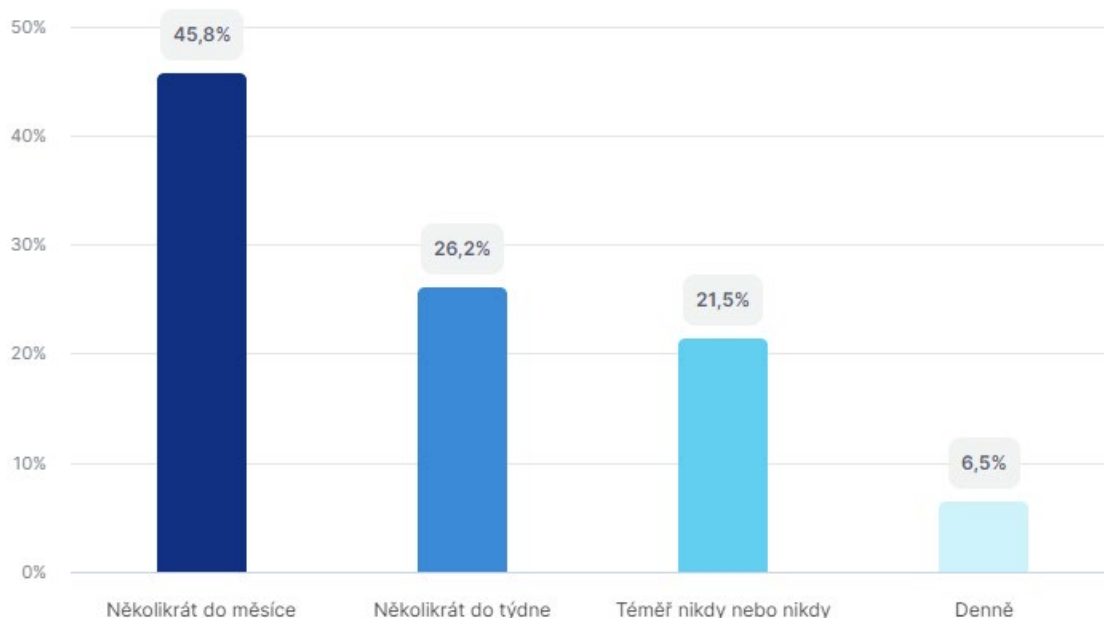


Zdroj: vlastní tvorba

V první otázce jsem se respondentů ptal na jejich preference při nákupech. Více než 54 % využívá obojí a rozhodují se podle situace. Pro 41,1 % je hotovost přežitek a nejraději by vše platili kartou. Na druhou stranu zde 4,7 % respondentů

odpovědělo, že nemá důvěru v nové technologie, a to hlavně v platební karty nebo internetové bankovníctví.

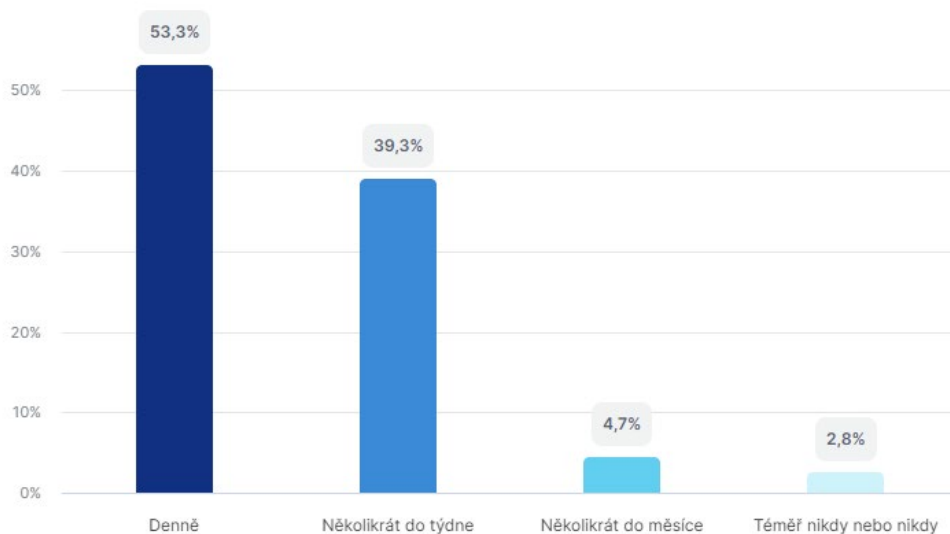
Graf č. 2 – Jak často platíte hotovostí?



Zdroj: vlastní tvorba

Z tohoto grafu je vidět, že nejvíce respondentů využije platbu v hotovosti párkrát do měsíce. Několikrát do týdne hotovost využije 26,2 % dotázaných. Ti, kteří odpověděli, že hotovost nevyužívají téměř nikdy nebo nikdy, tvoří podíl o 21,5 %. Druhým extrémem jsou dotazovaní, jež platí hotovostí denně. K této odpovědi se hlásí pouhých 6,5 % dotázaných.

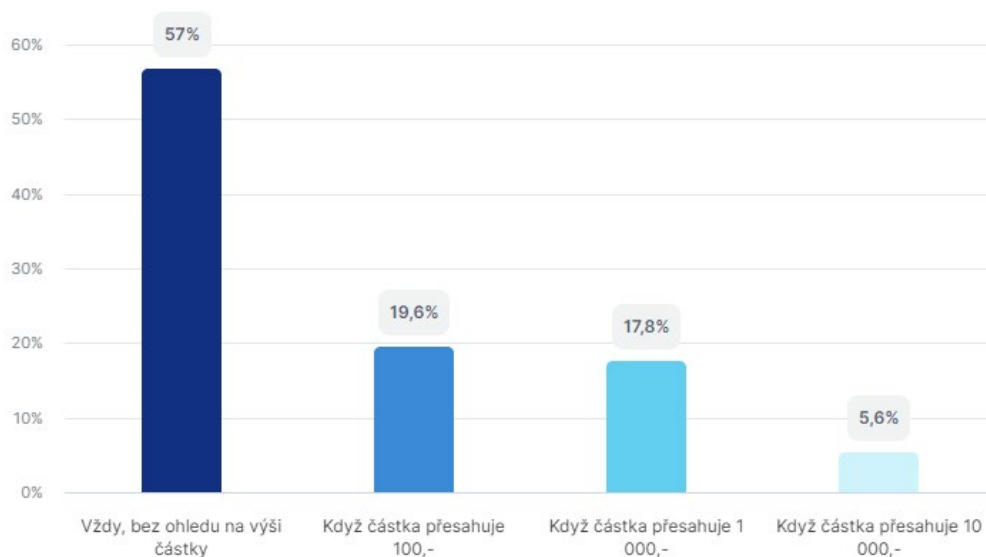
Graf č. 3 – Jak často platíte bezhotovostně?



Zdroj: vlastní tvorba

V porovnání s předešlým grafem je jednoznačné, že společnost obecně tíhne k využívání bezhotovostních plateb. V tomto případě 53,3 % platí kartou denně a pouhých 2,8 % neplatí kartou vůbec nebo téměř vůbec. Druhým nejsilnějším údajem je využití bezhotovostních prostředků několikrát do týdne. Tuto odpověď zvolilo o 13 % více respondentů než v předešlé otázce. Několikrát do měsíce zaplatí bezhotovostně 4,7 %.

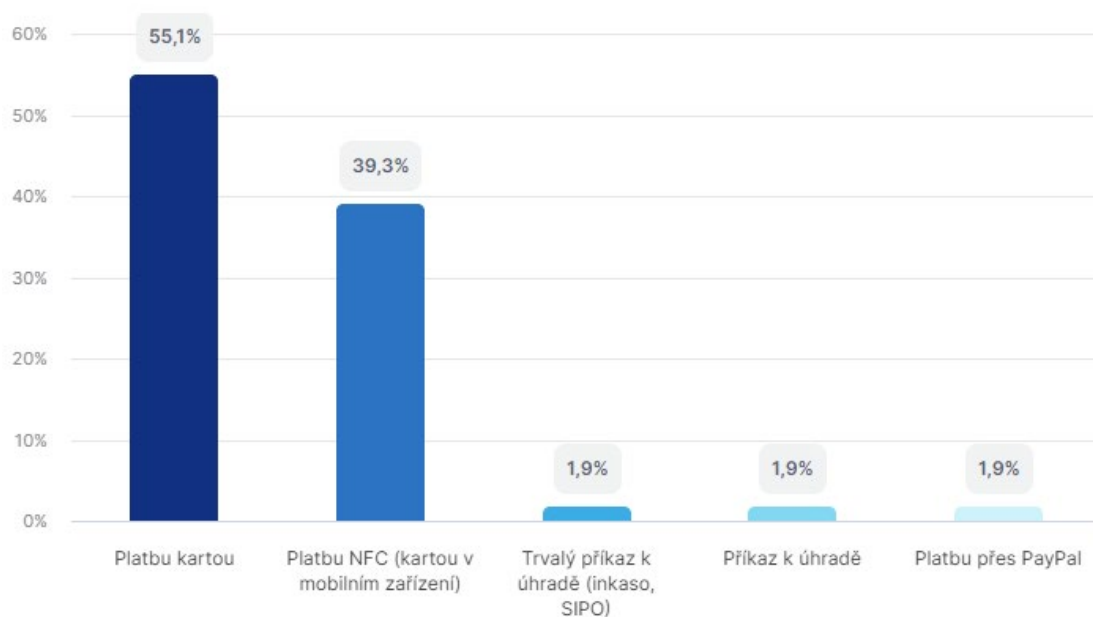
Graf č. 4 – Od jaké výše částky preferujete bezhotovostní platbu?



Zdroj: vlastní tvorba

Zajímalo mě, jestli existuje vztah mezi peněžní částkou a pravděpodobností, že jednotlivec zaplatí bezhotovostně. Z grafu vyplývá, že 57 % dotazovaných platí kartou bez ohledu na výši částky. Ovšem z dalších údajů lze vyčíst, že s vyšší částkou se zvedá i pravděpodobnost využití bezhotovostní operace.

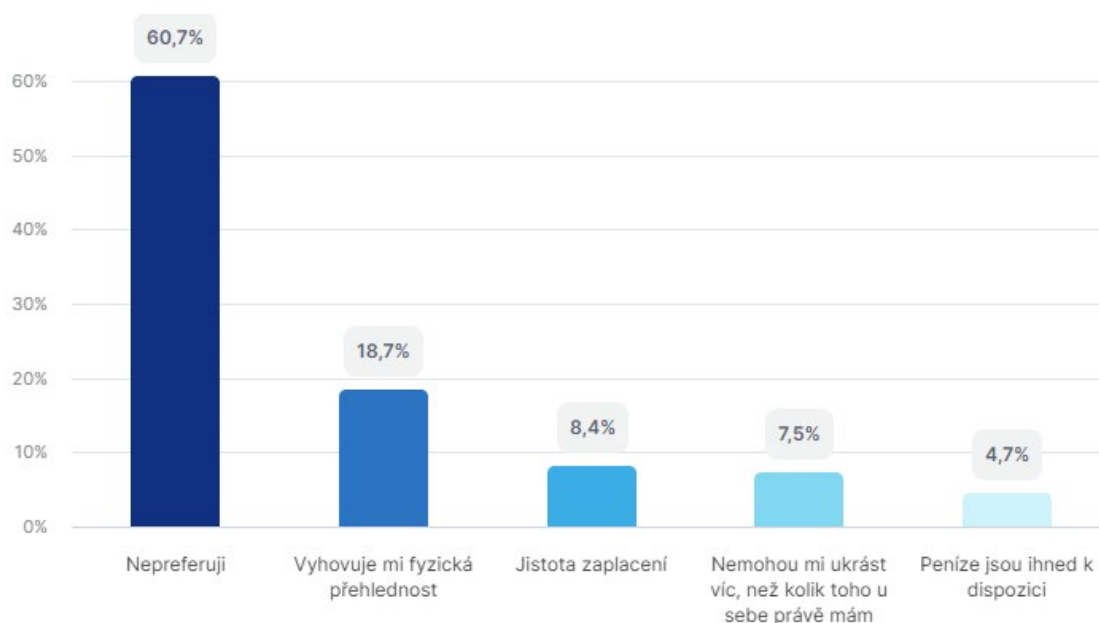
Graf č. 5 – Pokud platím bezhotovostně, preferuji nebo nejčastěji využívám:



Zdroj: vlastní tvorba

V jedné ze svých otázek jsem se ptal, jaké technologie jsou nejoblíbenější při bezhotovostní platbě. Výsledkem je, že přes 94 % dotazovaných použije platební kartu, ať už fyzickou nebo v mobilním zařízení. Trvalý příkaz, příkaz k úhradě a platba přes PayPal sdílí oblibu rovným dílem a to v 1,9 %.

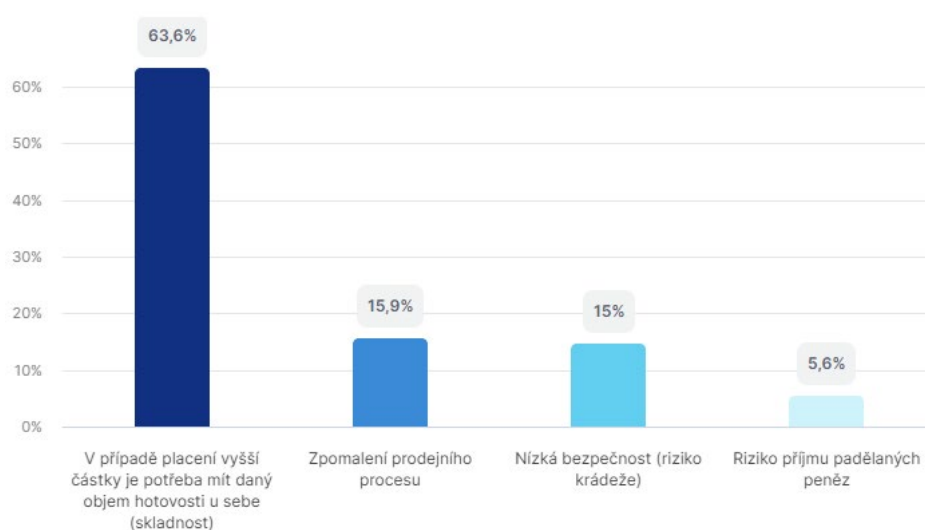
Graf č. 6 – Z jakého důvodu preferujete platbu hotovostí?



Zdroj: vlastní tvorba

Proč lidé preferují platbu hotovostí? V 60,7 % případů hotovost nepreferují. Ti, kteří ji preferují, tak v 18,7 % to je hlavně z důvodu fyzické přehlednosti. V 8,4 % případů lidé platí v hotovosti, aby se ujistili, že transakce opravdu proběhla a pro 7,5 % dotazovaných to představuje domnělou bezpečnost. Fyzické peníze chce mít po ruce 4,7 %.

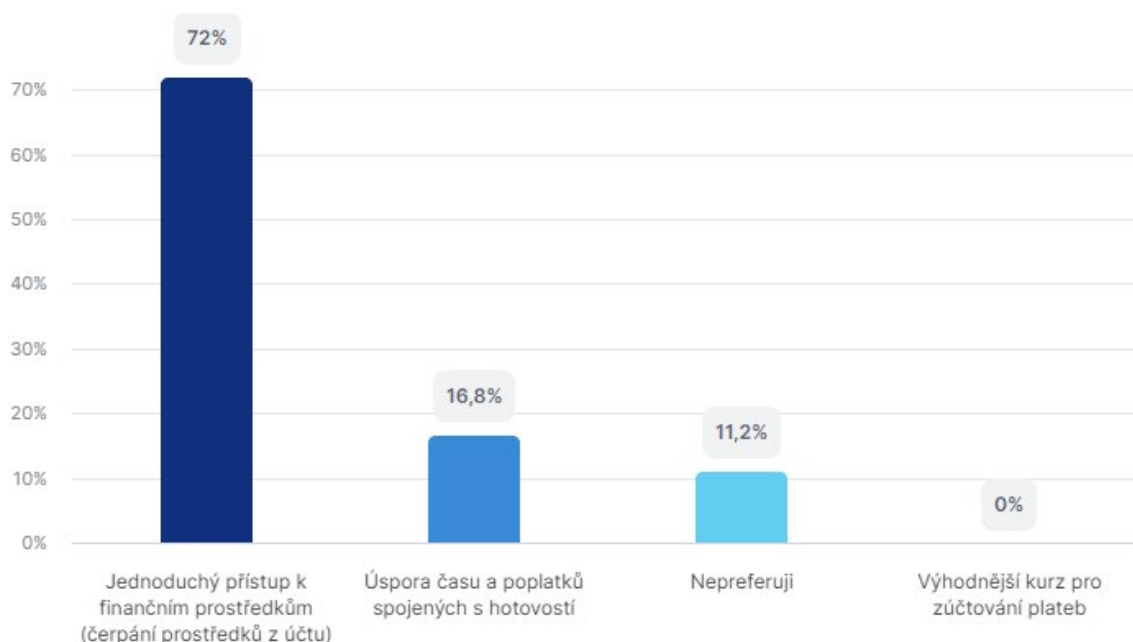
Graf č. 7 – Jaká je podle Vás největší nevýhoda při platbě hotovostí?



Zdroj: vlastní tvorba

V této otázce jsem zjišťoval, jaká je největší nevýhoda u fyzických peněz. Nejvíce respondentů (63,6 %) vnímá jako slabou stránku, že je potřeba nosit u sebe daný obnos peněz. Jedná se o validní argument, jelikož s rostoucí inflací by bylo potřeba u sebe nosit víc a víc peněz. Druhá nejčastější odpověď (15,9) je spojená se samotnou operací platby, která se kvůli přepočítávání bankovek a mincí zpomaluje. Ovšem rizika spojená s příjmem a platbou hotovostí jsou až na třetím a čtvrtém místě. Nebezpečí krádeže v anketě zaznamenalo 15 % dotazovaných a 5,6 % vnímá jako riziko příjem pozměněných nebo padělaných peněz. Tento údaj nepřímo podporuje tvrzení Marka Fryštáka a Evy Žatecké, že občané podceňují pravděpodobnost setkání s padělanými bankovkami.

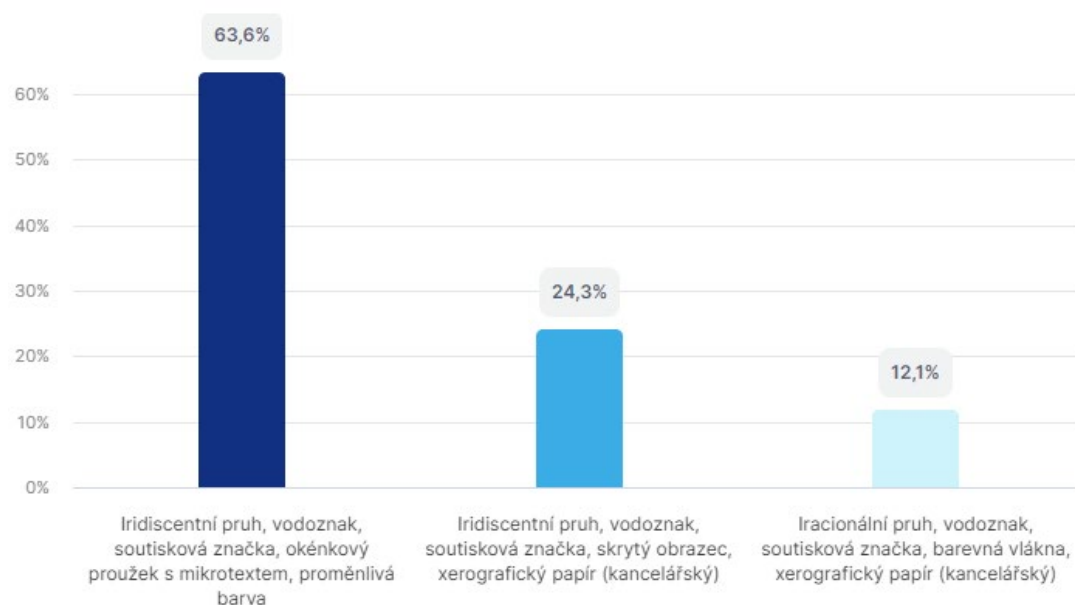
Graf č. 8 – Z jakého důvodu preferujete platbu bezhotovostně?



Zdroj: vlastní tvorba

Graf č. 8 vypovídá o důvodech preference bezhotovostních plateb oproti fyzickým penězům. V první řadě se jedná o pohodlnější transakci, jelikož potřebná částka se sama odečte z účtu po pouhém přiložení karty ke čtečce. Tuto možnost zaškrtno celkem 72 %. Částečně to souvisí i s druhou nejpopulárnější odpovědí, což je zrychlení prodejního procesu, kterou zaškrtno 16,8 % respondentů. Bezhotovostní platby nepreferuje 11,2 % a možnost výhodnějšího kurzu pro zúčtování plateb nevnímá žádný z respondentů jako výhodu.

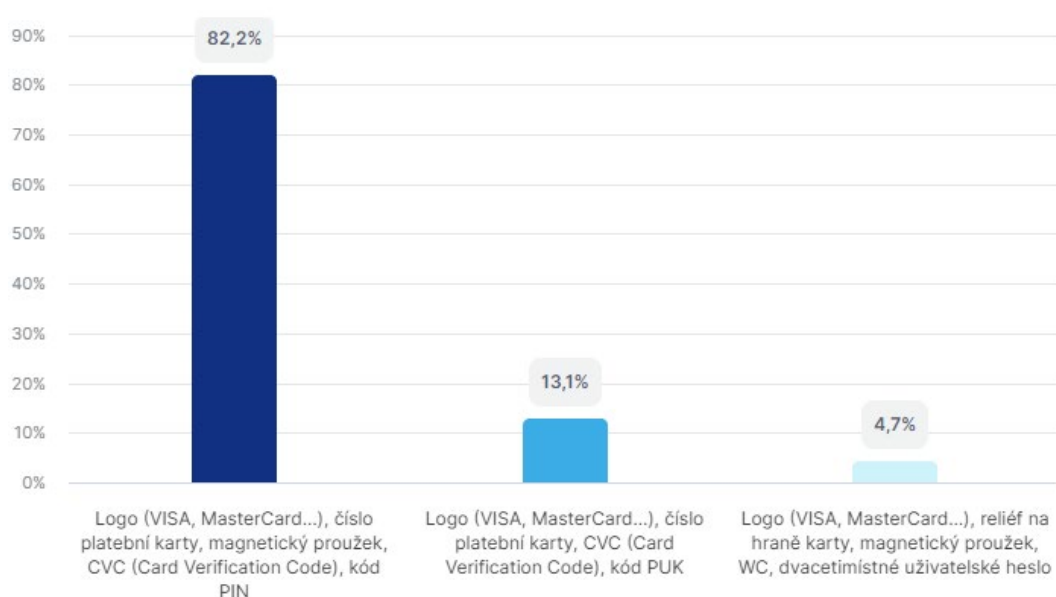
Graf č. 9 – Víte, co patří mezi nejčastější ochranné prvky bankovek?



Zdroj: vlastní tvorba

U této otázky jsem zjišťoval povědomí respondentů o ochranných prvcích bankovek. Přes 63 % odpovědělo správně a ví o ochranných prvcích bankovek. Další dvě možnosti obsahovaly kancelářský papír, což nepatří mezi ochranné prvky. Špatné možnosti tedy zvolilo celkem 36,4 % respondentů.

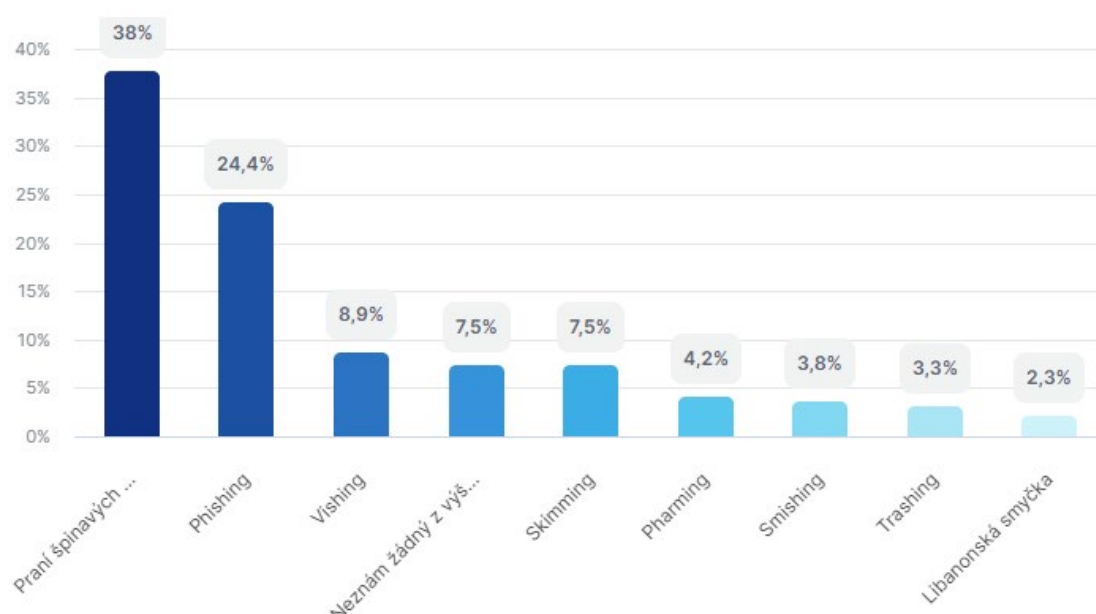
Graf č. 10 – Víte, co patří mezi nejčastější ochranné prvky platebních karet?



Zdroj: vlastní tvorba

Ochranné prvky platebních karet jsou známy více lidem. Správnou odpověď zde zaškrtnulo 82,2 % odpovídajících. Dle mého názoru to je zapříčiněno tím, že platební karty disponují méně, ale kvalitnějším zabezpečením. Bankovky jsou kvůli pokročilému vývoji technologii náchylnější k tvorbě padělků, tím pádem vyžadují komplexnější ochranné prvky. Menšina obsahující 17,8 % zvolila možnost nesprávnou.

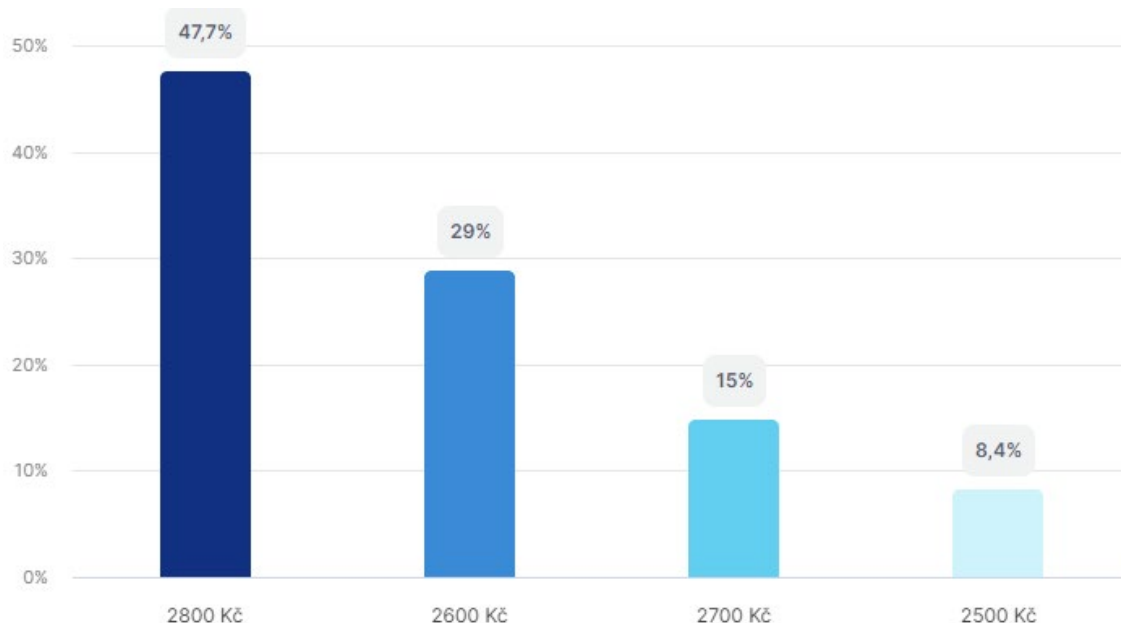
Graf č. 11 - Uměl byste říct, co je to:



Zdroj: vlastní tvorba

Znalost rizik a podvodů je prevencí pro bezpečnost platebního styku. Z tohoto grafu je patrné, že nejznámějším pojmem je praní špinavých peněz (38 %). Jako další se umístil phishing (24,4 %) a jeho alternativa vishing (8,9 %). Jednotlivců, kteří se neselekali s těmito pojmy nebo je neznají, je celkem 7,5 %.

Graf č. 12 - Za nákup ve Švýcarsku jsme kartou zaplatili 100 švýcarských franků (CHF). Naše banka k danému dni nabízela švýcarské franky za tyto kurzy: nákup 25 CHF/CZK, prodej 27 CHF/CZK. Jaká částka se nám za nákup strhne na bankovním účtu za předpokladu, že si banka účtuje za převod měn paušální poplatek 100 Kč?

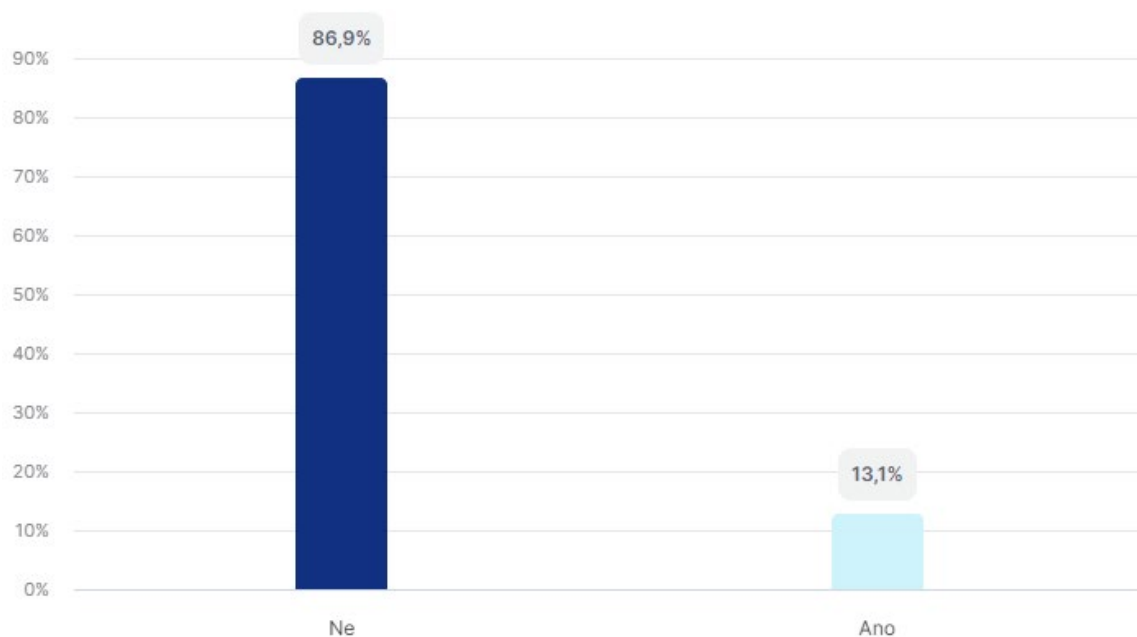


Zdroj: vlastní tvorba

Informovanost a znalost jsou klíčovými prvky bezpečnosti plateb. Důvěra k finanční instituci může klesnout, pokud nám naúčtuje neobvyklé a nečekané poplatky... ale jsou opravdu nečekané? Tato otázka měla za úkol vyhodnotit orientaci jednotlivce v nákupu nebo prodeji cizích měn.

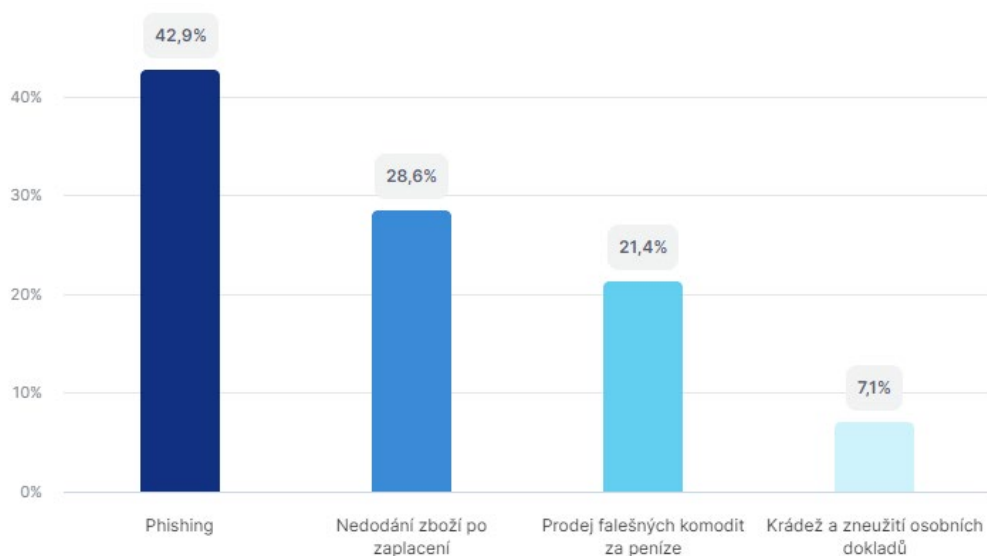
Jde o poměrně jednoduchou fiktivní úlohu, kterou úspěšně vyřešilo méně než 50 % respondentů. Přestože se jednalo o nákup v obchodě, tak při bezhotovostní operaci nám banka švýcarské franky prodávala, tudíž jsme i s poplatkem zaplatili 2800 Kč. Zbylých 52,3 % respondentů nezvolilo správnou odpověď a při zobrazení bankovního účtu by je mohl překvapit vyšší výdaj, než by původně očekávali.

Graf č. 13 - Stali jste se někdy obětí finančního podvodu?



Mezi dotázanými bylo celkem 13,1 % jednotlivců, kteří se stali obětí nějakého finančního podvodu. Na tuto otázku navazuje další, která byla s otevřenou odpovědí a oběti podvodu zde mohly napsat svou zkušenost a o jaký druh podvodu se jednalo. Odpovědí na tuto otázku bylo celkem 14, po přechtení každé z nich jsem identifikoval jednotlivé podvody a roztřídil je do následujícího grafu.

Graf č. 14 – Pokud jste se stali obětí podvodu, napište, o jaký typ podvodu se jednalo



Zdroj: vlastní tvorba

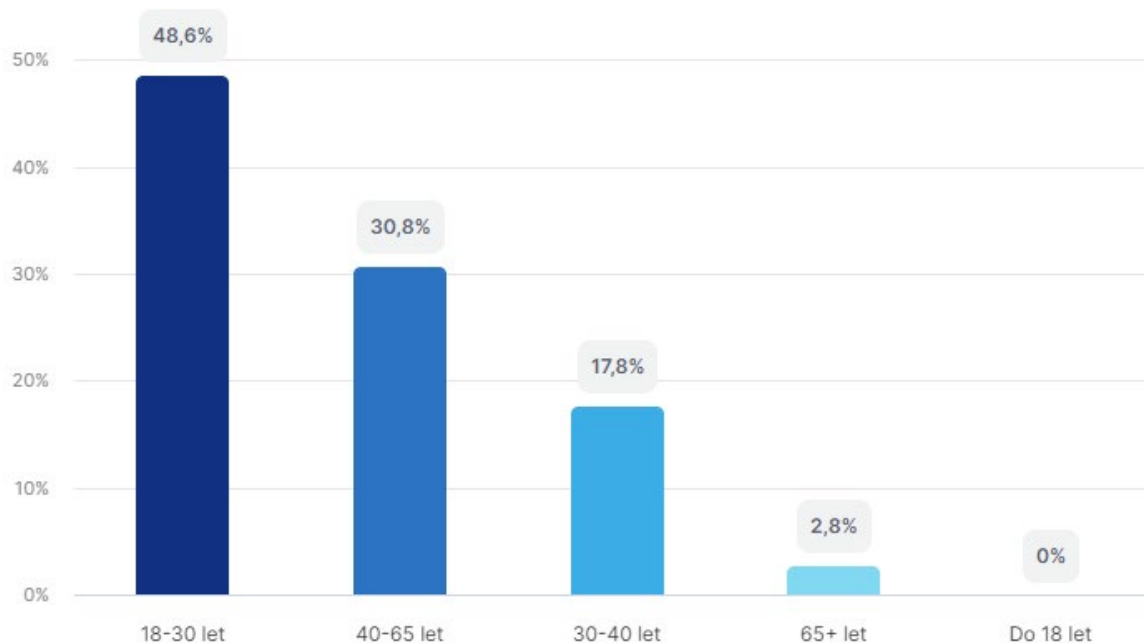
Phishingový útok je jedním z nejčastějších podvodů, což se potvrdilo v dotazníkovém šetření, kde tvoří celkem 42,9 % případů.

Následující praktikou je nedodání zboží spotřebiteli po provedení transakce (28,6 %). Zpravidla jde o fiktivní e-shopy, které jsou vytvořeny pouze za účelem nelegitimních praktik. V lepším případě mohou poškozeného připravit o drobnou finanční částku v podobě nákupu, v horších případech se jedná o phishingové a pharmingové stránky, které mohou získat osobní data spotřebitele.

Prodejce falešných komodit lze nalézt například na nádražích nebo tržnicích. Jejich cílem je oklamat oběť a prodat falešné zlato, případně falešný zlatý výrobek. Falzifikáty lze odhalit nepřírozenou barvou, rozměrem nebo váhou, ale nejlepší je se těmito „prodejci“ vyhnout a nakupovat pouze u důvěryhodných obchodníků. Falešné komodity tak zaujaly třetí místo s četností 21,4 %.

Poslední položkou je krádež peněženky na veřejnosti a následné zneužití odcizených dokladů, které se objevilo v 7,1 % odpovědí.

Graf č. 15 – Do jaké věkové kategorie patříte?

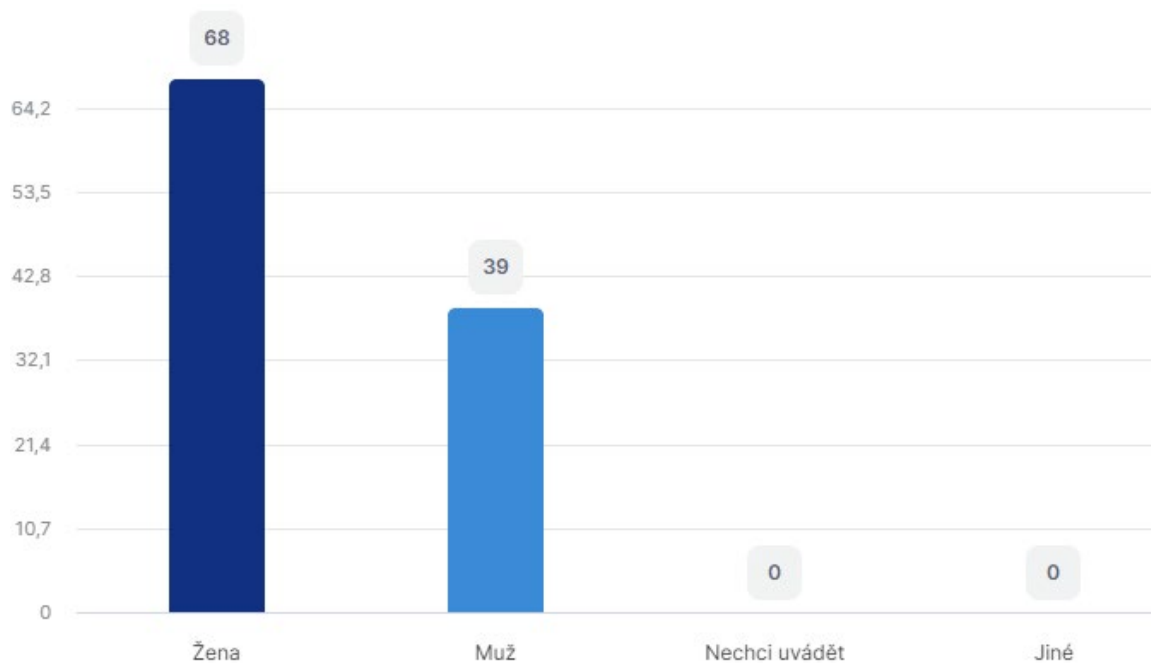


Zdroj: vlastní tvorba

Poslední tři otázky byly zaměřeny na demografické údaje. Tento graf popisuje věkové kategorie, které se podílely na vyplňování dotazníku. Mezi dotazovanými bylo 48,6 % do 30 let a 30,8 % mezi 40 až 65 lety. K předposlední věkové kategorii

30-40 let se přihlásilo 17,8 % respondentů a nejmenší zastoupení bylo osobami nad 65 let.

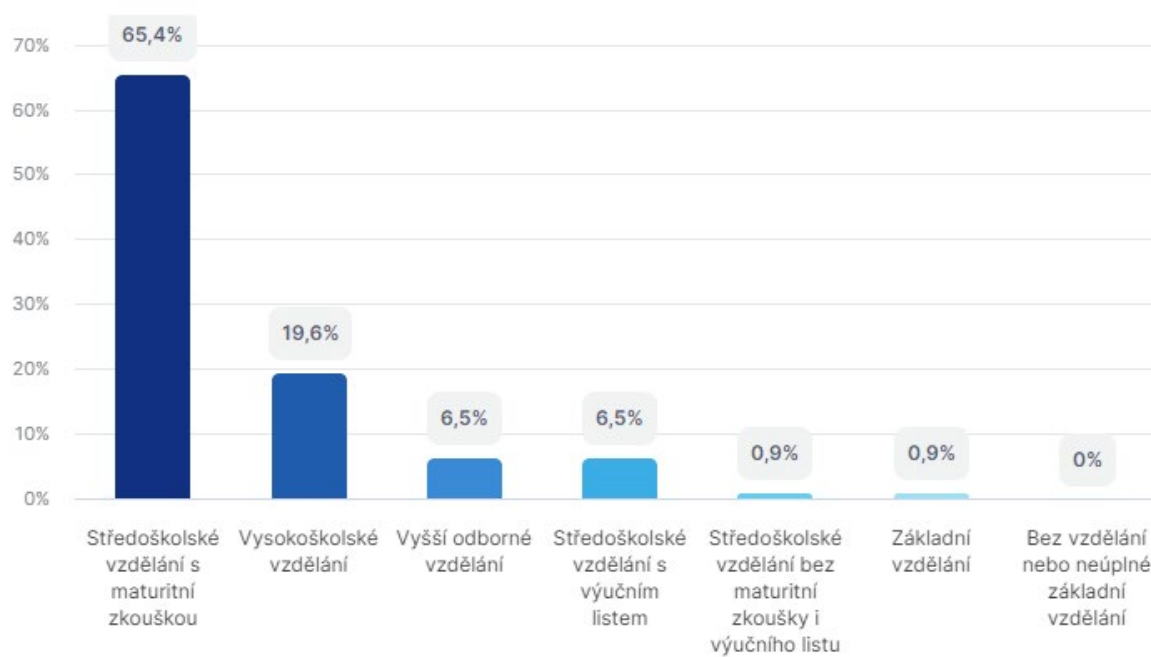
Graf č. 16 – Jaké je Vaše pohlaví?



Zdroj: vlastní tvorba

Do ankety se zapojilo celkem 68 žen a 39 mužů.

Graf č. 17 - Jaké je Vaše nejvyšší dosažené vzdělání?



Zdroj: vlastní výzkum a tvorba

V posledním grafu byli dotazovaní rozdělení podle dosaženého vzdělání. Nejčastěji se jednalo o respondenty se středoškolským nebo vysokoškolským vzděláním.

Vyhodnocení výzkumných předpokladů

V této krátké kapitole vyhodnotím stanovené výzkumné předpoklady, které jsem vypsals na začátek praktické části své bakalářské práce. Provádím tak na základě výše uvedených výsledků mého dotazníkového šetření.

Předpoklad č. 1 – Naprosté minimum respondentů nedůvěřuje bezhotovostní platbě.

V prvním grafu lze dohledat údaj, že 4,7 % dotazovaných preferuje hotovost, jelikož nedůvěřuje platbě kartou nebo přes internet. Výzkumný předpoklad č. 1 jsem tedy potvrdil.

Předpoklad č. 2 – Většina respondentů preferuje bezhotovostní platby.

Odpověď na tento předpoklad lze najít v grafech č. 4 a 6. V grafu č. 4 57 % odpovídajících preferuje bezhotovostní platbu bez ohledu na výši částky. Graf č. 6 říká, že 60,7 % respondentů nepreferuje hotovostní platbu, tím pádem je i předpoklad č. 2 potvrzen.

Předpoklad č. 3 – Většina respondentů zná ochranné prvky u bankovek a platebních karet.

Z grafu č. 10 vyplývá, že ochranné prvky platebních karet dokáže identifikovat 82,2 %. Zatímco u bankovek tomu je v 63,6 % případů. V obou případech se výzkumný předpoklad č. 3 potvrdil.

Předpoklad č. 4 - Osoby nad 40 let preferují spíše hotovostní platbu než bezhotovostní.

Pro vyhodnocení této hypotézy jsem vytvořil věkový filtr pro graf č. 6. Počet respondentů, kteří vyhovovali filtru (věk 40+) bylo celkem 33. Následně jsem

vytvořil graf, který jednoznačně shrne preference osob nad 40 let v oblasti platebního styku.

Graf č. 18 – Z jakého důvodu preferujete platbu hotovostí (40+)?



Z grafu je tedy patrné, že 22 osob nepreferuje platbu hotovostí. V relativních číslech je tato hodnota 66,7 %. Což vyvrací můj předpoklad, že respondenti nad 40 let preferují hotovostní platbu.

Předpoklad č. 5 - Nejčastějším podvodem, se kterým se respondenti setkali je phishing.

Poslední předpoklad závisí na výsledcích z grafu č. 14. Pokud se některý z dotazovaných stal obětí podvodu, tak se ze 42,9 % jednalo o phishingový útok. Phishing je tak nejčastějším podvodem, se kterým se respondenti setkali a potvrzuje to pátý výzkumný předpoklad.

Závěr

V dnešní době je patrné, že finanční služby procházejí rychlým technologickým pokrokem, který mění způsob, jakým lidé nakupují, platí a investují. Tyto inovace přinášejí řadu výhod pro spotřebitele, jako je pohodlnost, rychlost a dostupnost. Mobilní platby, internetové bankovníctví a digitální peněženky se stávají stále běžnějšími v každodenním životě. Nicméně s rostoucím využíváním technologií

ve finančních službách přichází také nová hrozba: zvýšené riziko kybernetických útoků a finanční kriminality. V teoretické části jsem shrnul nejčastější podvody spojené s platebním stykem. Jednoznačně nejrozšířenější je online trestná činnost v podobě phishingových útoků a jeho alternativních forem, jako jsou vishing nebo smishing. Naše finanční prostředky mohou být ohroženy i mimo online prostor například skimmingovým zařízením v bankomatu, popřípadě příjmem padělaných bankovek. Je tedy zřejmé, že s technologickým pokrokem ve finančních službách je nezbytné současně zdokonalovat bezpečnostní opatření a ochranu proti těmto podvodům. Česká národní banka se aktivně podílí na edukaci veřejnosti v rámci ochrany finančních prostředků a implementuje nejrůznější bezpečnostní prvky s cílem ochránit finanční systém České republiky.

V praktické části jsem si dal za cíl porovnat preference v rámci platebního styku a důvěru v ně. Ke sběru dat jsem zvolil dotazníkové šetření, kde jsem mimo jiné zjišťoval znalost respondentů v oblasti zabezpečení plateb, jestli preferují platbu hotovostní nebo bezhotovostní a zda se setkali s finančními podvody, popřípadě s jakými druhy.

Výsledky praktické části ukazují, že většina respondentů upřednostňuje bezhotovostní platby, především prostřednictvím platebních karet a zařízení podporujících technologii NFC. Zároveň se ukazuje, že s rostoucí částkou transakce roste i pravděpodobnost, že jedinec zvolí bezhotovostní platbu. Nicméně hotovost stále zůstává relevantní, především při placení menších částek. Výzkumné předpoklady byly vyhodnoceny na základě získaných dat. Potvrdilo se, že naprosté minimum respondentů nedůvěřuje bezhotovostním platbám, většina respondentů preferuje bezhotovostní platby a zná ochranné prvky u bankovek a platebních karet. Nicméně předpoklad o preferenci hotovostní platby u osob nad 40 let nebyl potvrzen, což naznačuje, že věk nemá výrazný vliv na preference platebních metod. Nejčastějším podvodem, se kterým se respondenti setkali, byl phishingový útok, což potvrzuje předpoklad o vysoké míře konfrontace s tímto typem podvodu. Tento výsledek zdůrazňuje důležitost prevence a osvěty v oblasti bezpečnosti platebního styku.

Celkově lze konstatovat, že bezpečnost platebního styku je důležitou problematikou, která ovlivňuje každodenní život jednotlivců i společnost jako celek. Výzkum provedený v rámci této práce poskytuje užitečné poznatky pro další

rozvoj bezpečnostních opatření a osvěty v oblasti platebních transakcí. Je zřejmé, že vzhledem k technologickému pokroku a rostoucímu výskytu trestné činnosti je nezbytné neustále zkoumat a aktualizovat bezpečnostní postupy a opatření, aby bylo možné chránit uživatele platebních systémů před riziky spojenými s platebním stykem.

Seznam použité literatury

Monografie

EISENHAMMEROVÁ, Monika a HEMŽSKÁ, Andrea. *Platební styk: studijní opora*. Pardubice: Univerzita Pardubice, 2014. ISBN 978-80-7395-869-5.

MÁČE, Miroslav. *Platební styk: klasický a elektronický*. Praha: Grada, 2006. ISBN 80-247-1725-5.

SCHLOSSBERGER, Otakar. *Platební služby*. Praha: Management Press, 2012. ISBN 978-80-7261-238-3.

ŠENKÝŘOVÁ, Bohuslava. *Bankovníctví*. Praha: Grada, 1997. ISBN 80-716-9464-9.

Trestné činy proti měně de lege lata a de lege ferenda. Marek Fryšták, Eva Žatecká. 2010.

Zákonná úprava

Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

Online. EUR - Lex. 2017. Dostupné z: https://eur-lex.europa.eu/eli/reg_del/2018/389/oj. [cit. 2024-03-07].

Zákon č. 129/2022 Sb. Zákon, kterým se mění zákon č. 370/2017 Sb., o platebním styku, ve znění pozdějších předpisů, a další související zákony.

Online. Zákony pro lidi. 2022. Dostupné z: <https://www.zakonyprolidi.cz/cs/2022-129>. [cit. 2024-03-07].

Zákon č. 136/2011 Sb. Zákon o oběhu bankovek a mincí a o změně zákona č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů

Zákon č. 136/2011 Sb. Zákon o oběhu bankovek a mincí a o změně zákona č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů. Online. Zákony pro lidi. 2011. Dostupné z: <https://www.zakonyprolidi.cz/cs/2011-136>. [cit. 2024-03-07].

Zákon č. 229/2002 Sb. Zákon o finančním arbitrovi. Online. Zákony pro lidi.

2002. Dostupné z: <https://www.zakonyprolidi.cz/cs/2002-229>. [cit. 2024-03-07].

Zákon č. 253/2008 Sb. Zákon o některých opatřeních proti legalizaci výnosů z

trestné činnosti a financování terorismu. Online. Zákony pro lidi. 2008. Dostupné z: <https://www.zakonyprolidi.cz/cs/2008-253>. [cit. 2024-03-07].

Zákon č. 368/2016 Sb. Zákon, kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, a další související zákony. Online. Zákony pro lidi. 2016. Dostupné z: <https://www.zakonyprolidi.cz/cs/2016-368#:~:text=368%2F2016%20Sb.-.Z%C3%A1kon%2C%20kter%C3%BDm%20se%20m%C4%9Bn%C3%AD%20z%C3%A1kon%20%C4%8D.,p%C5%99edpis%C5%AF%2C%20a%20dal%C5%A1%C3%AD%20souvisej%C3%ADc%C3%AD%20z%C3%A1kony>. [cit. 2024-03-07].

Zákon č. 370/2017 Sb. Zákon o platebním styku. Online. Zákony pro lidi. 2017. Dostupné z: <https://www.zakonyprolidi.cz/cs/2017-370>. [cit. 2024-03-07].

Zákon č. 527/2020 Sb. Zákon, kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, a další související zákony, zákony související s přijetím zákona o evidenci skutečných majitelů a zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů. Online. Zákony pro lidi. Dostupné z: <https://www.zakonyprolidi.cz/cs/2020-527>. [cit. 2024-03-07].

Zákon č. 69/2006 Sb. Zákon o provádění mezinárodních sankcí. Online. Zákony pro lidi. Dostupné z: <https://www.zakonyprolidi.cz/cs/2006-69>. [cit. 2024-03-07].

Webové stránky a elektronické zdroje

Co je NFC platba? Online. Moneta. 2023. Dostupné z: <https://www.moneta.cz/slovník-pojmu/detail/co-je-nfc-platba>. [cit. 2024-03-06].

Co je smishing. Online. Moneta. 2019. Dostupné z: <https://www.moneta.cz/slovník-pojmu/detail/smishing>. [cit. 2024-03-07].

Co to je praní peněz. Online. Česká národní banka. 2020. Dostupné z: https://www.cnb.cz/cs/o_cnb/cnblog/Co-to-je-prani-penez. [cit. 2024-03-07].

Elektronická peněženka. Online. Komerční banka. 2022. Dostupné z: <https://www.kb.cz/cs/podpora/slovník/vyrazy-zacinajici-na-e/elektronicka-penezenka#:~:text=Elektronick%C3%A1%20pen%C4%9B%C5%BEenka%20je%20webov%C3%A1%20nebo,pomoc%C3%AD%20e%2Dmailu%20a%20hesla.> [cit. 2024-03-06].

Investice ho stála 107 000 Kč. Online. Policie České republiky. 2023. Dostupné z: <https://www.policie.cz/clanek/investice-ho-stala-107-000-kc.aspx>. [cit. 2024-03-06].

Jak bezpečně využívat platební karty. Online. ČSOB. 2015. Dostupné z: <https://www.csob.cz/branteseroumem/zasady-bezpecneho-chovani/jak-bezpecne-vyuzivat-platebni-karty>. [cit. 2024-03-07].

Jsem nigerijský princ: Podvodníci s kryptoměnou útočí stále častěji. Online. Deník.cz. 2021. Dostupné z: <https://www.denik.cz/krimi/jsem-nigerijski-princ-podvodnici-s-kryptomenou-utoci-i-na-vysocine-20210905.html>. [cit. 2024-03-06].

Když Pavel či Babiš radí s investicemi. Podvodníci na internetu se zlepšují. Online. IDNES. 2024. Dostupné z: https://www.idnes.cz/zpravy/domaci/umela-intelligence-deep-fake-video-pavel-babis.A240209_192239_domaci_pukk. [cit. 2024-03-07].

Legislativa a metodika. Online. Finanční analytický úřad. 2020. Dostupné z: [https://fau.gov.cz/legislativa-a-metodika-459#:~:text=Z%C3%A1kladn%C3%ADm%20pr%C3%A1vn%C3%ADm%20p%5%99edpisem%20obsahuj%C3%ADc%C3%ADm%20pravidla,tak%C3%A9%20%E2%80%9EAML%20z%C3%A1kon%E2%80%9C\).](https://fau.gov.cz/legislativa-a-metodika-459#:~:text=Z%C3%A1kladn%C3%ADm%20pr%C3%A1vn%C3%ADm%20p%5%99edpisem%20obsahuj%C3%ADc%C3%ADm%20pravidla,tak%C3%A9%20%E2%80%9EAML%20z%C3%A1kon%E2%80%9C).) [cit. 2024-03-06].

Ochranné prvky 2000 Kč. Online. Česká národní banka. 2010. Dostupné z: <https://www.cnb.cz/cs/bankovky-a-mince/bankovky/ochranne-prvky-2000-kc/>. [cit. 2024-03-07].

Padělky 2023 Padělané a pozměněné bankovky a mince zadržené na území ČR. Online. Česká národní banka. 2024. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/verejnost/galleries/pro_media/konference_projevy/vystoupeni_projevy/download/kubelkova_20240304_padelky_2023.pdf. [cit. 2024-03-06].

Platím kartou. Online. PCI Standard. 2023. Dostupné z: <https://www.pcistandard.cz/pcidss/drzitel/#:~:text=Podvodn%C3%ADk%20vlo%C5%BE%C3%AD%20do%20%C5%A1t%C4%9Brbiny%20%C4%8Dte%C4%8Dky,si%20podvodn%C3%ADk%20zapamatuje%20nebo%20zaznamen%C3%A1>. [cit. 2024-03-07].

Počítačová kriminalita. Online. Policie České republiky. 2020. Dostupné z: <https://www.policie.cz/clanek/pomoc-obetem-tc-pocitacova-kriminalita.aspx>. [cit. 2024-03-06].

Podvod s investicemi. Online. Policie České republiky. 2023. Dostupné z: <https://www.policie.cz/clanek/podvod-s-investicemi.aspx>. [cit. 2024-03-07].

Podvodníci, kteří se vydávají za Policii. Online. YouTube. Dostupné z: <https://www.youtube.com/watch?v=rB0x09uAyyE>. [cit. 2024-03-07].

Právo na placení hotovostí v Ústavě? Vláda návrh označila za nadbytečný. Online. Seznam zprávy. 2023. Dostupné z: <https://www.seznamzpravy.cz/clanek/ekonomika-pravo-na-placeni-hotovosti-v-ustave-vlada-navrh-oznacila-za-nadbytecny-234676>. [cit. 2024-03-06].

Pravomoc a působnost. Online. Kancelář finančního arbitra. 2019. Dostupné z: <https://finarbitr.cz/cs/reseni-sporu/pusobnost-financniho-arbitra.html>. [cit. 2024-03-06].

Pravomoci bankovního dohledu. Online. Česká národní banka. 2024. Dostupné z: <https://www.cnb.cz/cs/dohled-financni-trh/vykon-dohledu/postaveni-dohledu/dohled-nad-uverovymi-institucemi/pravomoci-bankovniho-dohledu/>. [cit. 2024-03-07].

Sextortion emails: how to protect yourself. Online. National cyber security center. 2018. Dostupné z: <https://www.ncsc.gov.uk/guidance/sextortion-scams-how-to-protect-yourself>. [cit. 2024-03-07].

Skimming. Online. Policie České republiky. 2014. Dostupné z: <https://www.policie.cz/clanek/ncoz-skimming.aspx>. [cit. 2024-03-07].

Stal se obětí podvodného e-mailového útoku. Přišel o desítky tisíc. Online. Prachatický deník.cz. 2021. Dostupné z: <https://prachaticky.denik.cz/zlociny-a-soudy/stal-se-obeti-podvodneho-e-mailoveho-utoku-prisel-o-desitky-tisic-20210310.html>. [cit. 2024-03-06].

Šifrování dat. Online. ESET. 2019. Dostupné z: <https://www.eset.com/cz/firmy/firemni-reseni/sifrovani/>. [cit. 2024-03-07].

The revised Payment Services Directive (PSD2) and the transition to stronger payments security. Online. EUROPEAN CENTRAL BANK. 2018. Dostupné z: https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html. [cit. 2024-03-07].

Vishing a spoofing. Online. Policie České republiky. 2021. Dostupné z: <https://www.policie.cz/clanek/vishing-a-spoofing.aspx#:~:text=Fiktivn%C3%AD%20bankovn%C3%AD%20%C3%BA%C5%99edn%C3%ADk%20vystra%C5%A1%C3%AD%20r%C5%AFzn%C3%BDmi,pouze%20o%20do%C4%8Dasn%C3%A9%20bezpe%C4%8Dnostn%C3%AD%20opat%C5%99en%C3%AD..> [cit. 2024-03-06].

Víte, jak ochránit své peníze na internetu? Online. Moneta. 2019. Dostupné z: <https://www.moneta.cz/caste-dotazy/odpoved/vite-jak-ochranit-sve-penize-na-internetu>. [cit. 2024-03-07].

VÝROČNÍ ZPRÁVA O ČINNOSTI FINANČNÍHO ARBITRA ZA ROK 2022. Online. Kancelář finančního arbitra. 2023. Dostupné z: https://finarbitr.cz/galerie/tinymce/V%C3%BDro%C4%8Dn%C3%AD%20zpr%C3%A1va%20o%20%C4%8Dinnosti%20finan%C4%8Dn%C3%ADho%20arbitra%202022_1.pdf. [cit. 2024-03-06].

What Is Money Laundering? Online. Investopedia. 2024. Dostupné z: <https://www.investopedia.com/terms/m/moneylaundering.asp>. [cit. 2024-03-07].

What is phishing? Online. IBM. 2023. Dostupné z: <https://www.ibm.com/topics/phishing>. [cit. 2024-03-06].

What is vishing? Online. Terranova security. 2022. Dostupné z: <https://terrnovasecurity.com/what-is-vishing/>. [cit. 2024-03-06].

Seznam grafů, obrázků a tabulek

Tabulka č.1 – Padělané a pozměněné bankovky a mince	15
Obrázek č. 1 – SMiShingová zpráva.....	16
Graf č. 1 - Co z následujícího nejlépe charakterizuje vaše zvyklosti při placení za nákupy?.....	38
Graf č. 2 – Jak často platíte hotovostí?.....	39
Graf č. 3 – Jak často platíte bezhotovostně?.....	40
Graf č. 4 – Od jaké výše částky preferujete bezhotovostní platbu?.....	40
Graf č. 5 – Pokud platím bezhotovostně, preferuji nebo nejčastěji využívám....	41
Graf č. 6 – Z jakého důvodu preferujete platbu hotovostí?.....	42
Graf č. 7 – Jaká je podle Vás největší nevýhoda při platbě hotovostí?....	42
Graf č. 8 – Z jakého důvodu preferujete platbu bezhotovostně?.....	43
Graf č. 9 – Víte, co patří mezi nejčastější ochranné prvky bankovek?.....	44
Graf č. 10 – Víte, co patří mezi nejčastější ochranné prvky platebních karet?...	44
Graf č. 11 - Uměl byste říct, co je to.....	45
Graf č. 12 - Za nákup ve Švýcarsku jsme kartou zaplatili 100 švýcarských franků (CHF). Naše banka k danému dni nabízela švýcarské franky za tyto kurzy: nákup 25 CHF/CZK, prodej 27 CHF/CZK. Jaká částka se nám za nákup strhne na bankovním účtu za předpokladu, že si banka účtuje za převod měn paušální poplatek 100 Kč?.....	46
Graf č. 13 - Stali jste se někdy obětí finančního podvodu?.....	47
Graf č. 14 – Pokud jste se stali obětí podvodu, napište, o jaký typ podvodu se jednalo.....	47
Graf č. 15 – Do jaké věkové kategorie patříte?.....	48
Graf č. 16 – Jaké je Vaše pohlaví?.....	49
Graf č. 17 - Jaké je Vaše nejvyšší dosažené vzdělání?.....	49
Graf č. 18 – Z jakého důvodu preferujete platbu hotovostí (40+)?.....	51

Přílohy

Příloha č. 1 – Výhružný e-mail sextortion phishingu

„Urgentní bezpečnostní upozornění: Zjistena možná neoprávněná přístup

E-mail byl zařazen do složky Doručené na základě přesunu pomocí protokolu IMAP. V případě potíží doporučujeme zkontrolovat nastavení poštovních klientů.

Vážený/a xxxx,

s lítostí vám oznamuji, že došlo k bezpečnostnímu porušení týkajícímu se zařízení, která používáte pro internetové prohlížení.

Před několika měsíci jsem získal neoprávněný přístup k těmto zařízením a sledoval vaše internetové aktivity.

Nedávno se mi podařilo hacknout vaše e-mailové účty, včetně vašeho hesla: xxxx

Navíc jsem na všechna zařízení, která používáte k přístupu k e-mailu, nainstaloval trojský virus.

To bylo možné díky tomu, že jste klikli na odkazy ve svých e-mailových doručených složkách, což mi usnadnilo proniknout do vašeho systému.

Pomocí tohoto softwaru jsem získal přístup k různým funkcím vašich zařízení, jako je mikrofon, videokamera a klávesnice.

Take jsem získal a uložil vaše osobní informace, data, fotografie a historii prohlížení webu na svých serverech.

Kromě toho jsem získal přístup k vašim poselům, sociálním sítím, e-mailové korespondenci, historii chatu a seznamu kontaktu.

Abych zůstal nejspokojený, můj virus neustále obnovuje své podpisy, což znamená, že je neviditelný pro antivirový software.

Behem mého vyšetřování jsem zjistil, že často navštěvujete webové stránky pro dospělé a zabýváte se explicitním obsahem.

Podarilo se mi nahrát explicitní videa vás a vytvořit montáž, která ukazuje vaše intimní okamžiky a sebeuspokojování.

Pokud pochybujete o autenticnosti mych tvrzení, mohu snadno tyto videa sdílet s vašimi přáteli, kolegy a příbuznými, nebo je dokonce zveřejnit veřejně.

Verím, že je ve vašem nejlepším zájmu tomu zabránit, s ohledem na potenciální následky zveřejnění takového explicitního obsahu.

Proto navrhuji řešení: převést 500 USD na můj bitcoinový účet (podrobnosti jsou uvedeny níže), na základě směnného kurzu v době transakce.

Jakmile bude převod dokončen, okamžitě smažu veškerý kompromitující materiál.

Poté se naše cesty rozejdou a zaručuji vám, že deaktivuji a odstraním veškerý škodlivý software z vašich zařízení.

Můžete se spolehnout, že splním svou část dohody.

S ohledem na rozsáhlé informace, které o vás mám, a čas, který jsem venoval sledování vašich aktivit, považuji tuto nabídku za spravedlivou a rozumnou.

Pokud si nejste jisti, jak nakupovat a převádět bitcoiny, doporučuji použít vyhledávací pro pomoc.

Bitcoinový účet: bc1xxxxxywrj0hmhx2adkd8jppvkqc6wyx8g9u7xd

Prosim, nedelejte následující kroky:

Neodpovídejte na tento e-mail, protože jsem ho vytvořil ve vaši doručené složce a vygeneroval jsem návratovou adresu.

Nepokoušejte se kontaktovat policii nebo jiné bezpečnostní služby. Navíc neinformujte své přátele, protože mi bude snadné zjistit takové kroky díky mému ovládnutí vašeho systému. V takovém případě okamžitě zveřejním videa veřejně.

Je zbytečné se pokoušet mě najít, protože všechny transakce s kryptomenami jsou anonymní.

Preinstalování operačního systému nebo se zbavit vašich zařízení nebude účinné, protože videa již byla uložena na vzdálených serverech.

Několik věcí, o kterých se nemusíte obávat:

Okamžite obdržim váš prevod finančních prostředků, protože neustále sleduji vaše aktivity prostřednictvím mého trojského viru, který má schopnost vzdaleneho ovládání podobnou službě TeamViewer.

Jakmile bude prevod finančních prostředků dokončen, nemám zájem sdílet vaše videa. Nemám zájem komplikovat váš život dále, protože bych tak učinil již dříve, kdyby to byl můj záměr. Buďte si jisti, že všechno bude řešeno feroze.

Nakonec vám důrazně doporučuji vyhnout se podobným situacím v budoucnosti. Je moudré pravidelně měnit všechna svá hesla, abyste zvýšili svou online bezpečnost.“

Příloha č. 2 – Bezpečnost platebního styku – kvantitativní dotazník

1. Co z následujícího nejlépe charakterizuje vaše zvyklosti při placení za nákupy?
 - Většinu útrat platím hotově, nemám důvěru k placení kartou či přes internet
 - Hotovost je přežitek, kdyby to bylo možné, platil bych nejraději jen bezhotovostně
 - Je mi v zásadě jedno, jestli mám platit hotově či kartou, nosím u sebe obojí a rozhoduji se podle situace

2. Jak často platíte hotovostí?
 - Denně
 - Několikrát do týdne
 - Několikrát do měsíce
 - Téměř nikdy nebo nikdy

3. Jak často platíte bezhotovostně?
 - Denně
 - Několikrát do týdne
 - Několikrát do měsíce
 - Téměř nikdy nebo nikdy

4. Od jaké výše částky preferujete bezhotovostní platbu?
 - Vždy, bez ohledu na výši částky
 - Když částka přesahuje 100,-
 - Když částka přesahuje 1 000,-
 - Když částka přesahuje 10 000,-

5. Pokud platím bezhotovostně, preferuji nebo nejčastěji využívám:
 - Platbu kartou
 - Platbu NFC (kartou v mobilním zařízení)

- Platbu přes PayPal
- Příkaz k úhradě
- Trvalý příkaz k úhradě (inkaso, SIPO)

6. Z jakého důvodu preferujete platbu hotovostí?

- Peníze jsou ihned k dispozici
- Vyhovuje mi fyzická přehlednost
- Jistota zaplacení
- Nemohou mi ukrást víc, než kolik toho u sebe právě mám
- Nepreferuji

7. Jaká je podle Vás největší nevýhoda při platbě hotovostí?

- Nízká bezpečnost (riziko krádeže)
- Zpomalení prodejního procesu
- Riziko příjmu padělaných peněz
- V případě placení vyšší částky je potřeba mít daný objem hotovosti u sebe (skladnost)

8. Z jakého důvodu preferujete platbu bezhotovostně?

- Jednoduchý přístup k finančním prostředkům (čerpání prostředků z účtu)
- Úspora času a poplatků spojených s hotovostí
- Výhodnější kurz pro zúčtování plateb
- Nepreferuji

9. Víte, co patří mezi nejčastější ochranné prvky bankovek?

- Iracionální pruh, vodoznak, sůtisková značka, barevná vlákna, xerografický papír (kancelářský)
- Iridiscentní pruh, vodoznak, sůtisková značka, skrytý obrazec, xerografický papír (kancelářský)
- Iridiscentní pruh, vodoznak, sůtisková značka, okénkový proužek s mikrotextem, proměnlivá barva

10. Víte, co patří mezi nejčastější ochranné prvky platebních karet?

- Logo (VISA, MasterCard...), číslo platební karty, CVC (Card Verification Code), kód PUK
- Logo (VISA, MasterCard...), číslo platební karty, magnetický proužek, CVC (Card Verification Code), kód PIN
- Logo (VISA, MasterCard...), reliéf na hraně karty, magnetický proužek, WC, dvacetimístné uživatelské heslo

11. Uměl byste říct, co je to:

- Skimming
- Praní špinavých peněz
- Vishing
- Smishing
- Phishing
- Pharming
- Libanonská smyčka
- Trashing
- Neznám žádný z výše uvedených pojmů

12. Za nákup ve Švýcarsku jsme kartou zaplatili 100 švýcarských franků (CHF).

Naše banka k danému dni nabízela švýcarské franky za tyto kurzy: nákup 25 CHF/CZK, prodej 27 CHF/CZK. Jaká částka se nám za nákup strhne na bankovním účtu za předpokladu, že si banka účtuje za převod měn paušální poplatek 100 Kč?

- 2500 Kč
- 2600 Kč
- 2700 Kč
- 2800 Kč

13. Stali jste se někdy obětí finančního podvodu?

- Ano
- Ne

14. Pokud jste se stali obětí podvodu, napište, o jaký typ podvodu se jednalo

15. Do jaké věkové kategorie patříte?

- Do 18 let
- 18-30 let
- 30-40 let
- 40-65 let
- 65+ let

16. Jaké je Vaše pohlaví?

- Muž
- Žena
- Jiné
- Nechci uvádět

17. Jaké je Vaše nejvyšší dosažené vzdělání?

- Bez vzdělání nebo neúplné základní vzdělání
- Základní vzdělání
- Středoškolské vzdělání bez maturitní zkoušky i výučního listu
- Středoškolské vzdělání s výučním listem
- Středoškolské vzdělání s maturitní zkouškou
- Vyšší odborné vzdělání
- Vysokoškolské vzdělání