Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra obchodu a financí

Bakalářská práce

Bezpečnost platebních karet

Arina Zhelyenkova

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Arina Zhelyenkova

Podnikání a administrativa

Název práce

Bezpečnost platebních karet

Název anglicky

Security of Payment Cards

Cíle práce

Cílem práce je vymezit způsoby ochrany platebních karet (PK) v České republice, nastinit historii jejich vývoje v celém světě a přímo v ČR a zjistit současný stav ochrany PK ze strany držitele a ze strany banky, která karty vydala. Dílčím cílem práce je definování možných rizik při používání PK a metod ochrany proti podvodníkům. Vedlejším cílem práce je zhodnocení povědomí dotazovaných lidí v ČR o podvodech, spojených s využitim PK, a možnostech ochrany proti nim.

Metodika

Teoretická část práce je zpracována metodou literární rešerše a obsahuje popis historie vývoje PK a jejich druhů. Dále jsou vymezeny podvody, spojené s PK, a dostupné způsoby zajištění bezpečnosti PK.

Praktická část práce obsahuje analýzu výsledků dotazníkového šetření, zaměřeného na zkoumání povědomí dotazovaných lidí v ČR o podvodech, spojených s využitim PK, a možnostech ochrany proti nim. Vzhledem k omezeným možnostem autorky práce nemůže výběrový vzorek reprezentovat celou populaci ČR. Nicméně obsahuje dostatečný počet účastníků (100-200 osob), aby bylo možné udělat nějaké obecné závěry. Šetření je provedeno formou online dotazníku, vytvořeného na portálu Vyplnto.cz.

Je provedena segmentace respondentů podle toho, karty jaké banky používají, a podle socio-demografických charakteristik (pohlaví, věk, úroveň vzdělání, průměrný měsíční příjem atd.). Výzkumná otázka bude: Jaké skupiny respondentů jsou nejlépe informování o možnostech ochrany proti podvodům, spojeným s PK?

Ke zpracování a prezentaci odpovědí, získaných v rámci dotazníkového šetření, jsou použity matematicko-statistické a grafické metody.

V poslední části práce jsou vytvořena doporučení pro zvýšení bezpečnosti využiti PK a informovanosti lidí o metodách ochrany proti podvodníkům. Doporučení navazují na výsledky literární rešerše a dotazníkového šetření, aby reflektovala potřeby ochrany těch skupin lidí, kteří jsou podvodem ohroženy nejvíce.

Doporučený rozsah práce

30 – 40 stran

Klíčová slova

platební karta, internet, debetní karta, skimming, fishing, čip, pin

---

Doporučené zdroje informací

Juřík, Pavel. Patební karty: velká encyklopedie 1870-2006. Praha: Grada Publishing, 2006. ISBN 978-80-247-6391-0,

---

Předběžný termín obhajoby

2022/23 ZS – PEF

Vedoucí práce

Ing. Milan Ulrich

Garantující pracoviště

Katedra obchodu a financí

Elektronicky schváleno dne 10. 3. 2023

prof. Ing. Luboš Smutka, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 13. 3. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 14. 03. 2023

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Bezpečnost platebních karet" jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 15. března 2023 _____

Poděkování

Ráda bych touto cestou poděkovala vedoucím mé práce – panu Ing. Milanu Ulrichovi, za jeho oborné vedení a čas, který mi věnoval v rámci zpracování této práce. Rovněž děkuji všem participantům dotazníkového šetření, bez jejich odpovědí by provedení výzkumu v této práci nebylo možné.

Bezpečnost platebních karet

Abstrakt

Práce se zabývá zkoumáním problematiky bezpečnosti platebních karet v ČR. Cílem práce je vymezit způsoby ochrany platebních karet (PK) v ČR, nastínit historii jejich vývoje v celém světě a přímo v ČR a zjistit současný stav ochrany PK ze strany držitele a ze strany banky, která karty vydala. Pro účely naplnění tohoto cíle je v první části práce provedená literární rešerše. Vedlejším cílem práce je zhodnocení povědomí dotazovaných lidí v ČR o podvodech, spojených s využitím PK, a možnostech ochrany proti nim. Hlavní metodou praktické části práce je online dotazníkové šetření, kterého se zúčastnilo 137 mladých lidí z ČR. Z výsledků vyplývá, že respondenti s nižší úrovní vzdělání jsou nejméně informováni o možnostech pojištění PK; ženy méně než muži využívají jednotlivé způsoby kontroly spolehlivosti provozovatelů e-shopů. V návaznosti na tyto a další výsledky práce jsou vytvořena doporučení a návrhy.

Klíčová slova: platební karta, internet, debetní karta, skimming, fishing, čip, pin

Security of payment cards

Abstract

The work is focused ont the issue of the security of payment cards in the Czech Republic. The aim of the thesis is to define the methods of protection of payment cards (PK) in the Czech Republic, to outline the history of their development throughout the world and directly in the Czech Republic, and to find out the current state of protection of PK on the part of the holder and on the part of the bank that issued the cards. In order to fulfill this goal, a literature search is carried out in the first part of the thesis. A secondary objective of the work is to evaluate the awareness of the interviewed people in the Czech Republic about frauds connected with the use of PK and the possibilities of protection against them. The main method of the practical part of the work is an online questionnaire survey, in which 137 young people from the Czech Republic participated. The results show that respondents with a lower level of education are the least informed about PK insurance options; women use individual methods of checking the reliability of e-shop operators less than men. Based on these and other work results, recommendations and suggestions are made.

Keywords: payment card, internet, debit card, skimming, fishing, chip, pin

Obsah

1 Úvod

Platební styk je nejdůležitějším finančním nástrojem, který charakterizuje úroveň rozvoje státu. Efektivní a bezpečné provádění transakcí zvyšuje úroveň důvěry v národní měnu. Každá země se proto snaží co nejvíce začlenit inovace do ekonomiky, rozšířit nabídku poskytovaných služeb a zvýšit úroveň bezpečných bezhotovostních plateb. Platební karty zaujímají významné místo v různorodém systému platebních prostředků.

Bezpečnost zákazníků je pro banky klíčovým faktorem úspěchu. Zmíněný faktor výrazně ovlivňuje získávání, udržení či ztrátu zákazníků. Z tohoto důvodu je pro komerční banku rozhodující přijmout taková opatření, aby zajistila řádnou a účinnou ochranu klientů (Korauš a kol., 2017, s. 564).

Současná situace vyžaduje, aby komerční banky věnovaly bezpečnosti platebních karet mimořádnou pozornost. Soulad s potřebami a požadavky spotřebitelů, spokojenost zákazníků bank a komplexní péče o zákazníky jsou dnes středem pozornosti výzkumníků a bankéřů. Z tohoto důvodu tyto příslušné faktory představují důležitý marketingový nástroj pro mnoho společností, zejména těch, které působí na vysoce konkurenčních trzích (Belás, Demjan, 2014).

V souladu s rychlým růstem e-commerce v posledních několika desetiletích se na trhu platebních karet výrazně zvýšilo používání platebních karet pro online nákupy. Tato situace vedla k explozi podvodů s platebními kartami a stojí miliardy eur a dolarů ztrát v odvětví plateb kartami. Kromě přímých finančních ztrát způsobených podvody rostou obavy, že zvýšená pozornost veřejnosti k narušení dat a podvodům s platebními kartami může vést k obecnému podkopání důvěry spotřebitelů v elektronické platby.

Pochopení bezpečnosti proto prošlo významným vývojem. Kvůli nepřesnému hodnocení jejich osobního bezpečnostního stavu mají lidé tendenci podceňovat bezpečnostní prvky související s ochranou jejich finančních dat na internetu.

Tato práce poskytne několik pohledů na osobní bezpečnost a kvalitu zabezpečení platebních karet proti kybernetickým útokům. Výsledky práce mohou pomoci vydavatelům platebních karet a bankám i klientům používajícím platební karty, zejména ke zlepšení prevence před podvody a neoprávněným používáním platebních karet.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je vymezit způsoby ochrany platebních karet (PK) v České republice, nastínit historii jejich vývoje v celém světě a přímo v ČR a zjistit současný stav ochrany PK ze strany držitele a ze strany banky, která karty vydala. Dílčím cílem práce je definování možných rizik při používání PK a metod ochrany proti podvodníkům. Vedlejším cílem práce je zhodnocení povědomí dotazovaných lidí v ČR o podvodech, spojených s využitím PK, a možnostech ochrany proti nim.

2.2 Metodika

Teoretická část práce je zpracována metodou literární rešerše a obsahuje popis historie vývoje PK a jejich druhů. Dále jsou vymezeny podvody, spojené s PK, a dostupné způsoby zajištění bezpečnosti PK.

Praktická část práce obsahuje analýzu výsledků dotazníkového šetření, zaměřeného na zkoumání povědomí dotazovaných lidí v ČR o podvodech, spojených s využitím PK, a možnostech ochrany proti nim. Vzhledem k omezeným možnostem autorky práce nemůže výběrový vzorek reprezentovat celou populaci ČR. Nicméně obsahuje dostatečný počet účastníků (100-200 osob), aby bylo možné udělat nějaké obecné závěry. Šetření je provedeno formou online dotazníku.

Je provedena segmentace respondentů podle toho, karty jaké banky používají, a podle socio-demografických charakteristik (pohlaví, věk, úroveň vzdělání atd.). Výzkumná otázka bude: Jaké skupiny respondentů jsou nejlépe informování o možnostech ochrany proti podvodům, spojeným s PK?

Ke zpracování a prezentaci odpovědí, získaných v rámci dotazníkového šetření, jsou použity matematicko-statistické a grafické metody.

V poslední části práce jsou vytvořena doporučení pro zvýšení bezpečnosti využití PK a informovanosti lidí o metodách ochrany proti podvodníkům. Doporučení navazují na výsledky literární rešerše a dotazníkového šetření, aby reflektovala potřeby ochrany těch skupin lidí, kteří jsou podvodem ohroženy nejvíce.

3 Teoretická východiska

Platební karty jsou v dnešní době běžným platebním prostředkem, který používají miliony lidí po celém světě. Kdy se však platební karty objevily a proč se stály tak populární? Stručná historie platebních karet pomůže pochopit klíčové milníky jejich vývoje, včetně problémů, s nimiž se vývojáři karet potkávali.

3.1 Historie platebních karet

Platební karty jsou obvykle chápany jako produkt moderních technologií, ale první pokusy o jejich vytváření lze najít již v 19. století v Americe.

3.1.1 Úvěrové známky a karty

Kovové úvěrové známky Metal Charge Coins (Tokens), které se objevily kolem roku 1865, jsou považovány za nejstaršího předchůdce moderních platebních karet. Tyto známky měly evidenční čísla, spojena se jménem konkrétního zákazníka. Prodejce nepožadoval od kupujícího hotovost ani jiné formy peněz, ale evidoval číslo předložené známky (Hovorková, 2018). Útrata zákazníka byla připsána na úvěrový účet, a proto Metal Charge Coins lze považovat za určitý druh kreditní karty, spojené s úvěrovým účtem. Úvěrové známky byly akceptovány obchodníky až do 50. let 20. století (Hovorková, 2018; ČT24, 2014).

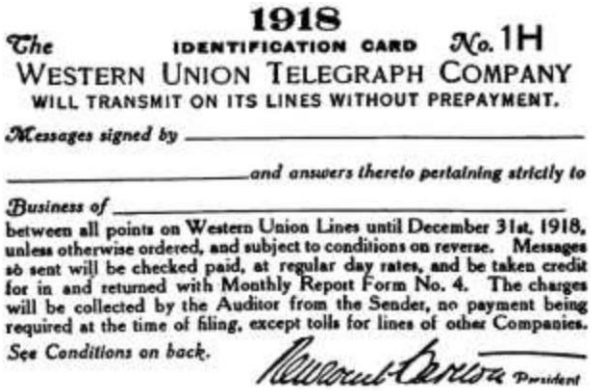
Vynález telegrafu v roce 1864 zrychlil rozvoj různých forem plateb, protože umožnil okamžitě předávat informace a převádět peníze. Rozkvět obchodu, dopravy a v neposlední řádě i tzv. Zlatá horečka zvýšily potřebu vylepšení platebních prostředků (ČT24, 2014).

Některé dopravní a telegrafní podniky se začaly nabízet svým nejdůvěryhodnějším a věrným zákazníkům papírové karty – Frank Card nebo Collect Card. Jednalo se o určitý druh firemní zákaznické karty, která umožňovala objednávat služby společností a platit za ně n fakturu následující měsíc (Hovorková, 2018).

Výzkumníci většinou shodují v tom, že první platební kartu v moderním slova smyslu vydala telefonní a telegrafní společnost **Western Union** a rok této události – 1914 – je považován za zrod moderní platební karty (Kalabis, 2015; Hovorková, 2018; Plischke, 2007). Zákazníci Western Union mohli s touto kartou (viz Obrázek 1) využívat služeb společnosti a na konci měsíce dostávali vyúčtování. Prakticky tedy šlo o věrnostní úvěrovou

kartu, která sloužila jako prvek věrnostního programu společnosti a konkurenční výhoda. Mnoho dalších společností napodobovaly kartu Western Union a některé katy měly dokonce plechovou podobu jako štítky v americké armádě (Plischke, 2007).

Obrázek 1: První platební karta Western Union Telegraph Company



1918

The IDENTIFICATION CARD No. 1H

WESTERN UNION TELEGRAPH COMPANY

WILL TRANSMIT ON ITS LINES WITHOUT PREPAYMENT.

Messages signed by _____

_____and answers thereto pertaining strictly to

Business of _____

between all points on Western Union Lines until December 31st, 1918, unless otherwise ordered, and subject to conditions on reverse. Messages so sent will be checked paid, at regular day rates, and be taken credit for in and returned with Monthly Report Form No. 4. The charges will be collected by the Auditor from the Sender, no payment being required at the time of filing, except tolls for lines of other Companies.

See Conditions on back.

President

Zdroj: Plischke, 2007

Kuznetsov (2007, s. 27) zmiňuje, že v roce 1914 první karty byly vydány nejen společností Western Union, ale i ropnou společností General Petroleum Corporation of Califronia (dnes je známa jako Mobile Oil). Tato karta mohla být využívána pro nákup ropných produktů, přičemž její vlastník získával značné výhody a slevy.

3.1.2 Vznik embosovaných karet

Nárůst počtu uživatelů karet si vyžádal vývoj systému pro účtování a evidenci tržeb pro každou vydanou kartu. Tak se objevila technologie **embosovaných karet** (vytlačení čísla a data expirace na přední straně karty a také jména a příjmení klienta). Písmo na embosované kartě umožňuje automatické sčítání údajů v mechanických snímačích u obchodníků – „*imprinter, zip zap machine*“ (Jílek, 2013, s. 525). Tato forma účtování operací se ukázala jako úspěšná a bez výraznějších změn přetrvala dodnes, i když se reliéfní písmo používá často již pouze ze zvyku.

V roce 1928 vyrobila společnost Farrugton Manufacturing se sídlem v Bostonu první embosované karty, které měly podobu kovových desek, na kterých byla vytlačena adresa. Tyto karty byly vydávány bonitním zákazníkům. Prodejce vložil takový štítek do imprinteru a otisk písmen na štítku se objevoval i na prodejním dokladu. V dalších letech se objevily takové prvky finančních úvěrových schémat jako minimální měsíční splátka dluhu, doba odkladu platby, tzn. bezúročné půjčky a mnoho dalšího (Kuznetsov, 2007, s. 27).

U embosovaných platebních karet však existovala snadná možnost zneužití. Zcizená nebo ztracená karta mohla být využívána i po nahlášení její odcizení či ztráty. Banky běžně dávaly kartu na tzv. stoplist až od půlnoci toho dne, kdy zákazník nahlásil ztrátu. Obchodníci běžně žádnou kontrolu karet podle stoplistu neprováděli, proto odcizená karta mohla bát zneužívána po dlouhou dobu (Jílek, 2013, s. 525).

Embosované karty nelze také označit z plnohodnotné platební prostředek, protože byly tzv. „klubovými" karty, které potvrzovaly příslušnost uživatele k určitému sektoru služeb (Kuznetsov, 2007, s. 27).

Rozvoj platebních karet byl dočasně pozastaven kvůli Velké hospodářské krize v roce 1929. Na konci 30. let 20. století se karty znovu objevily a vznikla první široce uznávána karta Universal Air Travel Plan, která byla používána k nákupu letenek. Ve 30. letech 20. století, s růstem automobilového průmyslu (čerpací stanice), rozvojem leteckých společností a obchodních společností pro nejuznávanější zákazníky, začaly společnosti nabízet 30denní odklad splátek, čemuž se dnes říká **bezúročné období** a bez kterého je těžké si představit moderní kreditní kartu (Kargina, 2009, s. 12). Rozvoj byl opět přerušen druhou světovou válkou, kdy americká vláda zakázala možnost čerpat z účtů úvěry (ČT24, 2014).

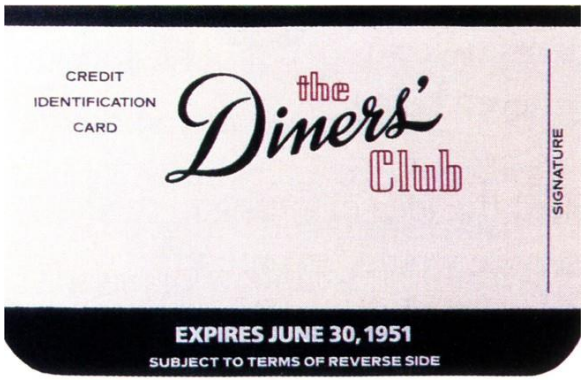
3.1.3 Karty Diners Club

V roce 1950 společnost **Diners Club** zavedla platební karty akceptované k platbě za služby v restauracích, hotelech a cestovních kancelářích. Ke vzniku karty Diners Club vedla náhodná událost, kdy pan Frank McNamara uspořádal obchodní večeři pro své klienty v restauraci Major's Cabin Grill v New Yorku. Poté McNamara zjistil, že zapomněl peněženku doma, proto nemohl zaplatit za večeři. V restauraci mu nabídli, aby zaplatil příště, protože byl známým obchodním ředitelem firmy Ford a Hamilton Credit Corporation (Juřík, 2005). Tato událost inspirovala McNamara vytvořit nějaký prostředek, který nahradí hotovost a odstraní potřebu nosit hotovost s sebou během cestování a návštěvy zábavních zařízení. Tak byla vytvořena karta Diners Club, které se následně začalo říkat „karty turistiky a zábavy" (Travel & Enterteinment Card, T&E Card). Jednalo se ve skutečnosti o první komplexní třístranné schéma dohody zahrnující vydavatele karty, obchodníky a držitele karty. V letech 1958-1959 s podobnými projekty vstoupily na trh společnosti American Express, Hilton Credit a další nebankovní organizace (Kuznetsov, 2007, s. 27).

Vzhledem k tomu, že T&E karty byly univerzálně použitelné a přinášely obchodníkům zvýšení tržeb, byl zaveden poplatek (provize) – cca 5-7 % z nákupu, který hradil obchodník (příjemcem karty) jejímu vydavateli. Také byl poprvé zaveden roční poplatek za vydání a správu karty ve výši 5 USD (Juřík, 2005).

Kreditní karty McNamara a Schneidera (partnera, který vstoupil do projektu) dostaly asi 200 vybraných zákazníků v únoru 1950. Tito klienti byli většinou osobní známí McNamara a Schneidera a pracovali v Empire State Building. Karty byly akceptovány 27 drahých restaurací a 2 hotely na Manhattanu. Obrat za první měsíc využití karet činil cca 2 tisíce USD a zisk 140 USD (Juřík, 2005). Na obrázku 2 je uvedena karta Diners Club.

Obrázek 2: Platební karta Diners Club



Zdroj: Hovorková, 2018

Několik měsíců poté byl McNamarovým přítelem Alfredem Bloomingdalem založen podobný systém – Dine and Sign v Los Angeles. Karta byla akceptována 25 restaurací a její obrat brzy dosáhl 150 tisíc USD. Po třech měsících fungování McNamara a Bloomingdale propojili své projekty, což vedlo k vytvoření celostátní Charge Card v USA. Diners Club se svým obchodním parterům ručil za závazky svých členů – majitelů karet a dostával provize z tržeb. Do roku 1952 se Diners Club rychle rostl a propojil již 330 restaurací v New Yorku, Los Angeles, Miami a Bostonu. Na konci roku 1952 s klubem pracovaly již více než tisíc restaurací, obchodů, hotelů, autopůjčoven a květinářství. Počet klientů činil 20 tisíc, obrat přesáhl 1 milion USD (Juřík, 2005).

Diners Club rostl také díky akvizicím. Společnost koupila jiného vydavatele karet Trip-Charge v roce 1956 a poté společnost Sheraton Central Credit Corporation v roce 1958. Karty Diners Club se stály prvními mezinárodními kartami, protože začaly je přijímat

podniky v Kanadě, Francii a na Kubě. V roce 1955 byly karty používány také k nákupům u leteckých společností. V roce 1956 činil počet uživatelů Diners Club cca 250 tisíc lidí, a proto neexistovala pro tuto kartu významná konkurence. V 60. leta se společnost pokusila rozšířit svoji spolupráci s bankami. Například v roce 1965 začala vydávat karty Diners Club britská banka Westminster Bank.

3.1.4 Karty American Express

Diners Club se stál bezpochybně gigantem ve světě platebních karet v 50.-60. leta 20. století. Na konci 50. let 20. století došlo však k růstu dalších významných společností v této oblasti. Za zmínku stojí projekty American Express, který začal vydávat papírové karty v roce 1958. Vizuálně se velice podobaly tehdejším cestovním šekům American Express (viz Obrázek 3). Karty rychle dosáhly úspěchu a již během prvního roku existence byly používány kolem 253 tisíc zákazníků. Na konci roku 1960 jejich počet činil již přes 750 tisíc a obrat převýšil 500 milionů USD. Firma však dost dlouho nedosahovala zisku, protože nebyla schopna účinně řídit riziko. Projekt byl ztrátový kvůli nespláceným úvěrům. Situace se změnila až v roce 1962, kdy George Waterse, později zvaný jako „otec karty“ zavedl opatření pro zvýšení tlaku na dlužníky a zvýšil roční poplatky (Hovorková, 2018).

Obrázek 3: Platební karty American Express

Zdroj: Hovorková, 2018

3.1.5 První bankovní karty a bankomaty

V letech 1951-1958 některé americké banky začaly vytvářet vlastní kartové systémy, ale jejich rozsah byl malý a karty byly místního charakteru (Kuznetsov, 2007, s. 28). **První bankovní kreditní karta** byla vydána Franklin National Bank of New York (Kalabis, 2015).

Významným projektem na trhu bankovních platebních karet se stála kreditní karta BankAmericard od Bank of America, vedoucí banky v oblasti spotřebních úvěrů.

V roce 1957 bylo ve Spojených státech 26 bank vydávajících karty, na jejichž programech se podílelo 754 tisíc držitelů karet a asi 11 tisíc organizací působících v oblasti obchodu. Objem obchodního obratu s použitím karet byl 40 milionů USD ročně (Kuznetsov, 2007, s. 28).

První bankomat se objevil v Londýně dne 27. června 1967. Uvedla ho Barclays Bank (Kalabis, 2015). V roce 1969 Chemical Bank v New Yorku uvedla do provozu první univerzální bankomat ATM (automated teller machine). Vzniku bankomatů však předcházela dlouhá leta, protože první žádost o registraci patentu automatického výplatního stroje podal Američán Luther G. Simjan v roce 1939. Název tohoto stroje byl Bankmatic. Pouze na začátku 60. let vynálezce přesvědčil First National Bank (Citibank) v tom, že modernizovaný stroj lze použit pro vkládání hotovosti a šeků. V praxi nebyl však tento přístroj téměř využíván (Kalabis, 2015).

3.1.6 Vznik mezinárodních platebních systémů

Tvrdá konkurence a rostoucí objemy peněžních převodů s rozvojem a plošným zaváděním informačních technologií vedly ke vzniku světově proslulých mezinárodních platebních systémů (mezinárodních karetních asociací) – Visa International, MasterCard International, JCB Card,

Visa International

Historie Visa International se začala v roce 1956, kdy Bank of America začala vydávat kreditní karty BankAmericard v Kalifornii. V roce 1970 americké banky, které tento projekt podpořily, vytvořily národní sdružení vydavatelů bankovních karet „BankAmericard“. V roce 1974 vznikla mezinárodní společnost „IBANCO“ („International Bank Company“ – Mezinárodní bankovní společnost, nebo IBC), jejímž hlavním úkolem byl vývoj systému vypořádání karet pomocí bankovních karet BankAmericard mimo území Spojených států amerických. V roce 1976 se mezinárodní společnost „IBANCO“ transformovala na společnost „Visa International“ a americká asociace vydavatelů bankovních karet „BankAmericard“ se stala známou jako „Visa USA“. Dnes jsou bankovní

karty „Visa International“ nejrozšířenější a přijímanou formou bezhotovostních plateb kartou po celém světě (Kuznetsov, 2007, s. 28).

MasterCard International

Projekt MasterCard začal koncem 40. let 20. století, kdy několik amerických bank začalo vydávat svým zákazníkům speciální platební doklad, který mohl být bankou použit jako záruka platby za náklady na nákupy jeho nositele v místních obchodech. V roce 1951 vyvinula Franklin National Bank v New Yorku pro tyto roky pokročilejší platební technologii, která umožnila začít vydávat první kreditní karty podobné moderním kartám. Následující desetiletí probíhala ve znamení rozvoje drobné, nebo, jak to nazval americký právník Andy Duke, „vesnické monopolizace“, tzn. kdy samostatná banka v každé lokalitě vydávala své karty a tvořila malou síť jejich oběhu s několika podniky obchodu a služeb sídlícími ve stejném bloku. Zlom nastal 16. srpna 1966, kdy skupina takových bank vytvořila Interbank Card Association (ICA), která se později stala MasterCard International. V roce 1988 MasterCard International podepsala smlouvu o spolupráci s EUROCARD International, která byla později přejmenována na Europe International. Tento krok umožnil MasterCard výrazně rozšířit počet účastníků v systému a rozsah karet, což posílilo její konkurenční pozici v evropském regionu a dalších částech světa. Později „MasterCard Int.“ převzala většinu kapitálu „Cirrus systém“, čímž dále posílila svou pozici na globálním trhu (Kuznetsov, 2007, s. 28).

Diners Club International

Mezinárodní platební systém Diners Club je jedním z prvních platebních systémů na světě a jedním z lídrů ve vydávání platebních karet pro cestování a zábavu (karty „T&E“ – „Travel & Entertainment“). Karty Diners Club lze dnes využívat jako běžné platební karty k nákupu zboží a služeb, výběr hotovosti v bankomatech. Výjimečnost karty je v tom, že nabízí mnoho benefitů a věrnostních výhod. Každému držiteli je poskytován soubor služeb, který zahrnuje všechny druhy pojištění, organizaci turistických a služebních cest, volný přístup do business center a salonků na největších letištích na světě, mezinárodní telefonní služby, různé bonusové systémy a nepřetržitá informační podpora. Karta je určena

lidem, kteří se věnují profesionální činnosti, mají stabilní, nadprůměrný příjem a poměrně často podnikají služební nebo turistické cesty.

JCB Card

Mezinárodní platební systém JCB Card byl založen japonskou společností JCB (Japan Credit Bureau) v roce 1961. Již od prvních let své existence začal tento platební systém poskytovat ekonomický odpor pokusům mezinárodních platebních systémů Visa a MasterCard dobýt japonský bankovní trh. Dnes je JCB lídrem na japonském trhu kreditních karet a aktivně se rozvíjí jako mezinárodní platební systém. JCB se zaměřuje především na spotřebitele vyšší a střední třídy s vysokými příjmy a diferencovanou poptávkou. JCB je jedinou společností v Japonsku, jejíž karty jsou mezinárodní. Od ostatních mezinárodních platebních systémů (Visa, MasterCard – všechny jsou mnohem větší než JCB) se přitom odlišuje zvýšeným důrazem na rozvoj jejich karet nejen jako platebního prostředku, ale jako prostředku pro přístup ke službám v oblasti cestovního ruchu a zábavy (JCB 2021).

Výše uvedené mezinárodní platební asociace vypracovávají obecná pravidla pro zúčtování transakcí, analyzují a upravují činnost celého řetězce finančních zúčtování. Kromě toho mateřské společnosti platebních asociací akumulují zdroje na zavádění nových technologií a také na vytváření a rozvoj informačních komunikací.

Výdaje asociací jsou hrazeny z příspěvků bank účastnících se mezinárodních platebních systémů v poměru k objemu jejich karetních transakcí.

Asociace plní následující funkce (Kuznetsov, 2007, s. 29):

- vydávání licencí na vydávání karet s logem společnosti,
- ochrana patentů a práv,
- vývoj norem a pravidel pro provádění operací,
- zajištění řádného fungování vnitrostátních a mezinárodních systémů automatizace a vyúčtování,
- měření finančních informací a převod plateb provizí účastníky systému,

- výzkum a analýza,
- vývoj nových platebních produktů,
- marketing, reklama a propagace produktů na trhu.

3.1.7 Vývoj v České republice

Československo se stálo první zemí socialistického bloku, kde byly přijímány platební karty, a byly to právě karty Diners Club (Juřík, 2005). Smlouvu s americkým klubem podepsala cestovní kancelář Čedok. S cílem zvýšit obrat a přilákat zahraniční zákazníky postupně začala přijímat i jiné karty (Juřík, 2012, s. 179).

V roce 1990 byla v Praze otevřena pobočka American Express, která převzala od Čedoku využití karet v síti obchodů (Juřík, 2012, s. 180).

Vlastní karty byly na území bývalého **Československa** vydány až v 90. leta, kdy Česká státní spořitelna zprovoznila první stovku bankomatů. V roce 1990 se Živnostenská banka stala členem asociace VISA a začala vydávat karty Visa Classic a později i Visa Business (Juřík, 2012, s. 180).

V roce 1991 bylo vytvořeno Mezibankovní sdružení pro platební karty, jehož zakladateli se stály Agrobanka, Komerční banka, Investiční banka, Tatrabanka, Poštovní banka a Všeobecná úvěrová banka. Cílem této organizace bylo vybudovat společný systém pro fungování platebních karet EuroCard / MasterCard (Švarcová, 2019).

„Boom“ platebních karet se na území Česka začal až v roce 1992 (ČT24, 2014). V roce 1994 zavedla Komerční banka a I. S. C. MUZO čipovou kartu, která byla určena pro firemní zákazníky, využívající služeb čerpacích stanic Tank Plus. V roce 1996 byl spuštěn projekt elektronické peněženky Clip. První magnetické čipové karty EMV byly zavedeny Komerční bankou v roce 2003 (Juřík, 2012, s. 185).

Bezkontaktní platební karty MasterCard PayPass se v ČR začaly být používány v roce 2011. V tomto roce se trochu později začala vydávat bezkontaktní karty Visa PayWay i Česká spořitelna. Karty byly akceptovány pouze některými prodejci – SPAR, Baumax, C&A, Cinema City. Citibank poté zavedla platební nálepky, které sloužily jako bezkontaktní čip a umožňovaly provedení plateb bezkontaktně (Juřík, 2012, s. 187).

3.2 Náležitosti moderních platebních karet a jejich typy

Moderní platební karty jsou považovány za nástroj bezhotovostního platebního styku, který používají fyzické osoby – občané a podnikatelé, zaměstnance na pracovních cestách, právnické osoby – obchodní korporace, obce, nadace, státní orgány atd. (Martišková, 2018).

Hlavním účelem platební karty je hospodaření s penězi bez nutnosti vždy mít u sebe hotovost. Platební karta umožňuje zaplatit bezhotovostně – v obchodech nebo přes internet. Hotovost lze však pomoci platební karty vybrat – v bankomatu nebo u pokladny. Většina platební karet je spojena s bankovním účtem. Proto hotovost lze na tento účet převést a následně použit tyto peníze k bezhotovostnímu pracovnímu styku pomoci platební karty. Pomoci karty lze také často využívat i půjčené prostředky – tzv. kontokorent nebo úvěr.

Funkcí každé platební karty je také identifikace jejího držitele a potvrzení jeho práv k provádění určitých operací souvisejících s používáním karty (Kuznetsov, 2007, s. 31). Každá platební karta musí obsahovat následující údaje (Švarcová, 2019):

- jméno držitele karty nebo určitý identifikační údaj např. rodné číslo, podpis majitele),
- označení vydavatele karty,
- číslo karty,
- doba platnosti karty,
- záznam dat – např. magnetický proužek, mikročip, laserový záznam.

Existuje mnoho vlastností, podle kterých lze platební karty klasifikovat. Například podle materiálu, ze kterého jsou karty vyrobeny: karty z papíru / kartou, karty z plastu, karty z kovu. Dnes jsou nejrozšířenější plastové karty.

Na základě mechanismu vypořádání jsou (Kuznetsov, 2007, s. 32):

- karty, založené na dvoustranném systému – historicky starší, vznikly na základě dvoustranných vztahů mezi účastníky vypořádání, kdy je držitelé karet mohou využívat k nákupu zboží v uzavřených sítích kontrolovaných vydavatelem karty,

- karty, založené na mnohostranném systému – poskytuje držitelům karet možnost nakupovat zboží na úvěr u různých obchodníků, kteří uznávají údaje karty jako platební prostředek.

Podle vydavatelů lze karty dělit na:

- bankovní – karty jsou nejčastěji vydávány bankami,
- nebankovní – karty mohou být vydávány jinými, nebankovními subjekty, mezi nejznámější patří American Express a Diners Club (SBK, 2012).

3.2.1 Karty podle typu elektronického záznamu dat

Podle typu elektronického záznamu dat na platební kartě lze uvést následující klasifikaci:

- karty s magnetickým proužkem
- čipové karty,
- hybridní karty,
- laserové karty.

Karty s magnetickým proužkem jsou historicky nejstarší karty. Magnetický proužek je umístěn na zadní straně karty. Nevýhodou této karty je možnost využití karty bez nutnosti zadávat PIN kód a riziko zfalšování podpisu, který je jediným a často nekontrolovatelným prvkem bezpečnosti (Polouček, 2006, s. 185). V současné době lze pozorovat trend odchodu od této technologie. Například MasterCard chce jako první systém platebních karet ukončit vydání karet s magnetickým proužkem a do roku 2029 již nebudou žádné nové karty tuto technologii ukládání dat (EditorCZ MasterCard, 2021). V České republice se karty s magnetickým proužkem již téměř nepoužívají kvůli rozšíření modernějších technologií – čipových karet.

Čipové karty se poprvé objevily v roce 1978. Data jsou u těchto karet umístěna v mikročipu. U telefonních předplatných karet se využívá jednodušší verze mikročipu – paměťová karta. U bankovních karet jsou využívány náročnější technologie – mikroprocesorové karty. Karty s takovými čipy lze programovat, měnit nebo odstraňovat

uložené údaje. Kromě údajů o držiteli karty obsahuje takový čip také informace o zůstatku na účtu klienta, proto při placení kartou není nutné přímé spojení s bankou pro zjištění aktuálního stavu. Mikroprocesorové karty zároveň zaručují nejvyšší míru ochrany (Dvořák, 2005, s. 374).

EMV je zkratka pro Europay, MasterCard a Visa – globální standard pro vzájemnou spolupráci čipů. EMV karty, které obsahují čip, ztížily padělání platebních karet.

Hybridní karty jsou vybaveny magnetickým proužkem i čipem, proto mohou být používány v terminálech obou typů – které podporují čip a které jsou vybaveny čtečkou proužku (Dvořák, 2005, s. 374).

Laserové karty byly vytvořeny v 80. letech 20. století. Tyto karty fungují podobně jako kompaktní disky. Vzhledem k vysoké ceně výroby samotné karty a využití technického zařízení pro čtení karet tohoto typu, jsou tyto karty na trhu nevyužívány (Dvořák, 2005, s. 375).

3.2.2 Karty podle typu zúčtování

Podle typu zúčtování lze vymezit karty debetní, kreditní a předplacené.

Většina karet je debetních. Jsou přímo spojeny s běžným účtem majitele karty. Peníze, které využívá majitel prostřednictvím této platební karty, jsou většinou jeho vlastní peníze, které má k dispozici na svém účtu. Nicméně majitel může často využit možnost kontokorentu, tj. jít do minusu.

Kreditní karty umožňují držitelům bankovních karet v souladu s podmínkami smlouvy s vydavatelem provádět transakce ve výši poskytnutého úvěrového rámce a v rámci výdajového limitu stanoveného vydavatelem, platit za zboží a služby a/nebo přijímat hotovost.

Předplacené platební karty jsou určené jejímu držiteli k provádění transakcí, ale nejsou vázaný na žádný konkrétní účet v bance a jsou většinou anonymní. jejichž vypořádání provádí úvěrová instituce – vydavatel svým vlastním jménem. Karty osvědčují právo držitele předplacené karty požadovat od úvěrové instituce – vydavatele, platbu za zboží (práce, služby, výsledky duševní činnosti) nebo vydání hotovosti (Moneta, 2023).

V poslední době se postupně do samostatného typu vyčleňují specifické prémiové karty, určené zpravidla vysoce bonitním klientům. Tento typ platebních karet je považován za nejprestižnější a vyznačuje se větším minimálním vkladem, vysokými náklady na jejich otevření a údržbu a také vyšším úvěrovým limitem v kombinaci se snadným získáváním hotovosti. Zástupci výkonných BPC jsou dnes „zlaté“, „platinové“ a „prémiové“ karty. Řada bank umožňuje u výše uvedeného typu karet přečerpání úvěrových prostředků – kontokorent (Kuznetsov, 2007, s. 32).

3.2.3 Karty podle způsobů použití

Podle povahy použití jsou karty určené jednotlivcům, rodinám, zaměstnancům podniku.

Rodinná karta se vydává rodinným příslušníkům osoby, která uzavřela smlouvu a která je odpovědná za účet. V tomto případě je možné schéma, kdy k jednomu bankovnímu účtu mají přístup dvě nebo více karet s různými identifikačními čísly. Osoba, která uzavřela smlouvu s vydavatelskou bankou, si přitom může nakládání s prostředky na tomto účtu regulovat dle vlastního uvážení. Může například nastavit limit pro použití finančních prostředků pro každou z karet „připojených“ k bankovnímu účtu.

Podniková karta je vydána právnické osobě. Na základě této karty mohou být vydávány jednotlivé karty vybraným osobám (vedoucím zaměstnancům, manažerům a dalším osobám). Obvykle jsou založeny osobní účty propojené s firemním účtem. Odpovědnost vůči bance za firemní účet náleží organizaci, nikoli jednotlivým majitelům firemních karet. Firemní karty jsou obvykle spojeny s různými výhodami v oblasti cestování, dopravy, obchodu (Kuznetsov, 2007, s. 33). Podnikové karty mohou být také označeny jako firemní, služební nebo business karty. Označení „služební karty“ se používá zejména pro platební karty, které jsou určeny k úhradě výdajů, spojených se služební cestou (Dvořák, 2005, s. 383).

Platební karty lze rozdělil podle územní příslušnosti na mezinárodní (působící ve dvou nebo více zemích), národní / tuzemské (působící ve stejné zemi), místní (používané na určitém území státu nebo v jedné konkrétní instituci). Poplatky, spojené s tuzemskými karty jsou obvykle nižší než u karet mezinárodních, a jsou zde obvykle nižší požadavky na bonitu zákazníka (Dvořák, 2005, s. 382). Většina platebních karet, které jsou dnes běžně používány

spotřebiteli, jsou mezinárodní. Je to umožněno díky využití mezinárodních platebních systémů, jako jsou Visa, MasterCard.

Karty se vydávají na omezenou dobu (časově omezené) nebo jsou neomezené (jsou však extrémně vzácné). Většina karet má označenou dobu, do kdy karta platí. Uživatel karty má obvykle právo na prodloužení karty. Bankovní instituce v ČR zpravidla zajišťují automatické prodloužení platnosti karty a vydávají kartu novou. Klient pak je požádán, aby se dostával na pobočku banky a vyzvednul kartu novou. Někdy jsou karty doručovány kurýrem nebo poštou, což je z hlediska zákazníka pohodlnější. Z důvodu bezpečnosti je doručení karty osobně do rukou zákazníka vhodnější.

Z přehledu historie platebních karet a jejich druhů je patrné, že platební karty se v průběhu desetiletí značně vyvíjely. Ale velké množství konkurenčních standardů a jejich nerovnoměrné rozšíření po celém světě způsobily, že karty jsou zranitelné pro kreativní podvodníky (Gold, 2014, s. 12). Stejně, jako karty prošly určitým vývojem, legislativa ve vztahu k platebnímu styku se v průběhu času měnila. Jednou z důležitých oblastí právní úpravy je bezpečnost a ochrana uživatelů platebních karet.

3.3 Legislativa ve vztahu k ochraně plateb kartou

U platebních služeb, nabízených elektronicky, vč. plateb kartou, je vysoké riziko podvodu (Evropská komise, 2017). Na bezpečnost plateb kartou je kladen velký důraz zejména vzhledem k tomu, že tento typ plateb je jedním z nejčastějších způsobů úhrady za zboží a služby.

Podvody spojené s platebními kartami vyvolávají různé reakce u obětí – od zklamání a silného hněvu až po nedůvěru vůči bance, která „umožnila“ podvod uskutečnit. Důvěryhodnost je základním determinantem efektivního a stabilního bankovnictví, proto se v dnešní době bezpečný rozvoj stal skutečnou a naléhavou záležitostí v mnoha zemích světa (Štitilis, Klišauskas 2015; Kriviņš 2015).

Vzhledem k tomu je důležité vyvíjet v právní rámec, který zohledňuje a minimalizuje rizika podvodů v oblasti platebních styku. Jak uvádí ČNB, „*jedním z cílů legislativy v oblasti*

platebního styku je proto maximálně snižovat riziko zneužití platebních karet a předejít podvodům.“ (ČNB, 2021).

Zákon č. 370/2017 Sb., o platebním styku, je základním právním předpisem, upravujícím používání a manipulace s platební kartami v ČR. Tento zákon navazuje na příslušné předpisy EU. Bezpečnost v oblasti platebního styku je upravena §221 - §225 zákona č. 370/2017 Sb. V oblasti bezpečnosti zákon stanoví pravidla pro hlášení bezpečnostních a provozních incidentů, rizik a podvodných jednání. Dále jsou v zákony definovány podmínky, kdy je vhodné použit tzv. silné ověření uživatele.

3.3.1 Informační povinnost poskytovatelů platebních služeb v ČR

Hlášení bezpečnostních a provozních incidentů musí provést poskytovatel platební služby, a to bez zbytečného odkladu po jeho zjištění (§221 zákona č. 370/2017 Sb.). Incident musí být nahlášen elektronicky orgánu dohledu, tj. České národní bance (ČNB). ČNB pak o tomto hlášení informuje Evropský orgán pro bankovnictví a Evropskou centrální banku. Poskytovatel platební služby musí také o incidentu informovat uživatele služby, jemuž může v důsledku tohoto incidentu vzniknout újma na jmění. Zároveň musí být uživateli poskytnuta informace o tom, jak odvrátit tuto újmu.

Poskytovatel platebních služeb má také povinnost informovat ČNB o všech bezpečnostních a provozních rizicích, jímž je vystaven, a také o zavedených mechanizmech řízení těchto rizik (§221 zákona č. 370/2017 Sb.). Poskytovatel musí informovat o podvodních jednáních, které zaznamenal v oblasti platebního styku. Souhrnnou podobu těchto informací pak ČNB předává Evropskému orgánu pro bankovnictví a Evropské centrální bance.

Je patrné, že zákon o platebním styku v ČR upravuje oblast bezpečnosti především tak, že naznačuje různé informační povinnosti. Jedná se o povinnost poskytovatelů platebních služeb vůči ČNB a povinnost ČNB vůči evropským orgánům. Trendy v oblasti bezpečnosti plateb kartou jsou průběžně pro celou EU sledovány Evropskou centrální bankou (ČNB, 2021). V souvislosti s tím lze tvrdit, že kvalitní informace o rizicích a podvodech jsou velmi důležité pro možnost vývoje bezpečnostní politiky a zvýšení ochrany účastníků platebního styku.

3.3.2 Silné ověření uživatele

Silné ověření uživatele platební služby je jedním z důležitých nástrojů bezpečnosti v oblasti platebních styku, který by měl snižovat riziko zneužívání odcizených dat a platebních karet. Využití tohoto nástroje je zakotveno v českém zákoně, který navazuje na související evropská nařízení. Silné ověření uživatele je dle §223 zákona č. 370/2017 Sb. založeno na použití alespoň dvou z těchto prvků: *„a) údaje, který je znám pouze uživateli, b) věci, kterou má uživatel ve své moci, c) biometrických údajů uživatele.“* (Česko, 2017). Tyto prvky tvoří tři kategorie:

- znalost: údaje, které zná pouze uživatel, jsou např. heslo, PIN, odpověď na kontrolní otázku, obrázky na výběr,

- držba: věc, kterou má uživatel k dispozici, například jeho mobilní telefon, platební karty, fyzický token,

- inherence: biometrickým údajem může být otisk prstu nebo rozpoznání obličeje. Je třeba zde upozornit na to, že biometrické údaje jsou citlivé osobní údaje dle článku 9 GDPR, proto jeho zpracování podléhá speciálním právním předpisům (Gardlíková, 2019).

Minimální úroveň silného ověření uživatele je dvoufaktorová, a proto při provedení platby online již nestačí pouze zadání ověřovacího kódu CVV jako to bylo možné dříve (Bartoň Studio, 2021).

Dle §223 zákona č. 370/2017 Sb. poskytovatel platební služby má právo použit silné ověření uživatele v následujících případech: *„jestliže plátce a) přistupuje ke svému platebnímu účtu prostřednictvím internetu, b) dává platební příkaz k elektronické platební transakci, c) provádí jiný úkon, který je spojen s rizikem podvodného jednání v oblasti platebního styku, zneužitím platebního prostředku nebo informací o platebním účtu, nebo d) požaduje informace o platebním účtu prostřednictvím poskytovatele služby informování o platebním účtu.“* (Česko, 2017). V praxi je dvoufaktorové ověření uživatele vyžadováno například při online přístupu k platebnímu účtu, při provedení elektronické platební transakce nebo při jakékoli jiné činnosti, spojené s placením na dálku, a kde existuje riziko podvodu nebo zneužití dat (ČNB, 2021).

Předpisy a provozní pravidla týkající se podvodů s platebními kartami představují značnou zátěž pro komunitu vydavatelů karet. Vydavatelé karet jsou proto vysoce motivováni identifikovat oblasti zranitelnosti v systému a prosazovat nástroje pro prevenci podvodů (Korauš a kol., 2017, s. 564). Specifikovat podvody, s nimiž se mohou uživatelé potkat při placení kartou, je třeba specifikovat dále.

3.4 Podvody, spojené s platebními kartami

Podvody s kreditními a debetními kartami se za posledních několik let výrazně změnily. Pryč jsou časy, kdy podvodníci používali jednoduché skimmingové techniky – s mikrokamerami u bankomatů k zaznamenání PIN, aby získali přihlašovací údaje ke klonování karet. Před třiceti lety podvodníci aktivně klonovali tehdejší kreditní karty a vyráběli je. Dnešní podvodníci sbírají přihlašovací údaje ke kartám a související informace pomocí různých technik. Problém, kterému čelí průmysl platebních karet a jeho uživatelé je závažný. Problémem je, že podvody s kartami dnes přicházejí v mnoha různých podobách, a moderní počítačová kriminalita související s kartami výrazně přesahuje možnosti většiny organizací v oblasti bezpečnostních systémů (Gold, 2014, s. 15).

Na stránkách vývojářů software Dynamics 365 Fraud Protection – cloudového řešení, které pomoci umělé inteligence pomáhá zvyšovat identifikovat podvody a snížit jejich dopady, **podvod s platební kartou** je definován jako nejběžnější typ krádeže identity a zahrnuje neoprávněné použití účtu platební karty. Neoprávněné použití je důsledkem toho, že karta byla fyzicky odcizená, elektronicky odcizená (pomoci skimovacího zařízení nebo malwaru) nebo zakoupena na dark webu (Microsoft, 2022).

Bhatla a kol. (2003, s. 4-5) tvrdí, že podvody s platebními kartami lze obecně rozdělit do tří kategorií:

- tradiční podvody s kartami (odcizené karty, zneužití karet, akvizice, imitace a falešné účty),
- podvody související s podnikáním (tajné dohody s dealery a triangulace),
- podvody související s internetem (klonování stránek, generování kreditních karet a falešné stránky obchodníků).

3.4.1 Skimmingové techniky

Skimmingové techniky patří mezi tradiční a nejjednodušší podvody s kartami. Jde o okopírování údajů z magnetického proužku platební karty v bankomatu, automatu pro nákup jízdenek, tankovacích stojanů, při platbě u obchodníka, v hotelu atd. Skimming spočívá v několika krocích.

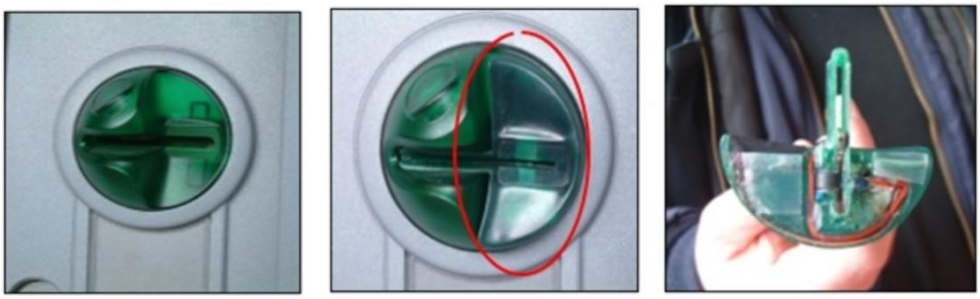
Zaprvé, podvodník instaluje speciální zařízení na vstupní otvor pro vložení karty bankomatu nebo jiného čtecího zařízení. Toto zařízení zkopíruje příslušná data na flash disk, který následně bude podvodníkem vyjmut, nebo předá je dálkově – přes Wifi, Bluetooth (CZ Protect, 2022). Příklad skimmovacího nástavce v otvoru bankomatu typu Wincor Nixdorf je uveden na obrázku 4. Je patrné, že vstup pro platební kartu je značně zúžen. Ve štěrbině vpravo se nachází magnetická hlavička – nelegální čtečka.

Obrázek 4: Skimmovací nástavec v otvoru bankomatu typu WN

Zdroj: Policie ČR, 2022

Skimmovací nástavce zelené barvy, které se instalují v bankomatech typu NCR, je vidět na obrázku 5. Lze zde také všimnout zúžení otvoru pro kartu.

Obrázek 5: Skimmovací nástavec v otvoru bankomatu typu NCR



antiskimm. nástavec pravý antiskimm. nástavec osazený nelegální čtečkou

Zdroj: Policie ČR, 2022

Za druhé, podvodník zjišťuje PIN kód karty, a to pomoci instalované mikrokamery nebo imitace klávesnice. Policie ČR (viz Obrázek 6) uvádí, že mikrokamery jsou často umístěny v reproduktorech, horní nebo dolní části obrazovky, bočních tělech bankomatu, a jsou ukryty v liště. Nejdražším případem je zaměření klávesnice termokamerou poté, co zákazník odejde od bankomatu (CZ Protect, 2022).

Obrázek 6: Minikamery, nainstalované v bankomatech

Zdroj: Policie ČR, 2022

Přes to, že skimmingová zařízení patří k historicky starým podvodům s platebními kartami, stále se s nimi lze v praxi setkat. Odhalit přítomnost skimmingového zařízení se stává stále obtížněji kvůli rozvoji výrobních technologií. Mohou být vyráběny ze stejného materiálu, jako bankomaty, nebo vyrobeny pomoci 3D tiskáren (Policie ČR, 2022).

3.4.2 Odcizení údajů ze spotřebitelských profilů v e-shopech

Podvody s platebními kartami vedou ke ztrátě peněz spotřebitelů a také mají velmi negativní dopady na maloobchodníky, pokud byl podvod spáchán na webu elektronického prodejce. Dnes jsou rozšířené případy, kdy podvodník odcizí údaje spotřebitelů o jejich platebních kartách, které jsou uloženy v účtech, založených na webových stránkách e-shopů. Podvody, cílené na online maloobchodníky, lze klasifikovat do pěti typů (Microsoft, 2022):

- podvody s aplikacemi: cizí osoba získá přístup k osobním údajům spotřebitele v aplikaci prodejce, a poté na jeho jméno založí nový účet, využívající platební údaje tohoto spotřebitele,

- podvod na dálku bez použití: cizí osoba získává údaje spotřebitele přes dark web nebo fyzickým odcizením platební karty, které využije k provedení podvodných objednávek,

- podvod s předstíranou identitou: osoba používá úmyslně nepravdivé údaje k založení kreditní karty a poté s ní proveden nákup dříve, než si poskytovatel karty uvědomí podvod,

- podvod s převzetím účtu: podvodník získává přístup k účtu spotřebitele, změní si doručovací adresu a požádá o náhradní platební kartu,

- přátelský podvod: spotřebitel si zakoupí produkt a poté požádá o vrácení peněz; bude tvrdit, že objednávku nikdy neprovedl nebo objednaný produkt neobdržel.

3.4.3 Phishing na online bazarech

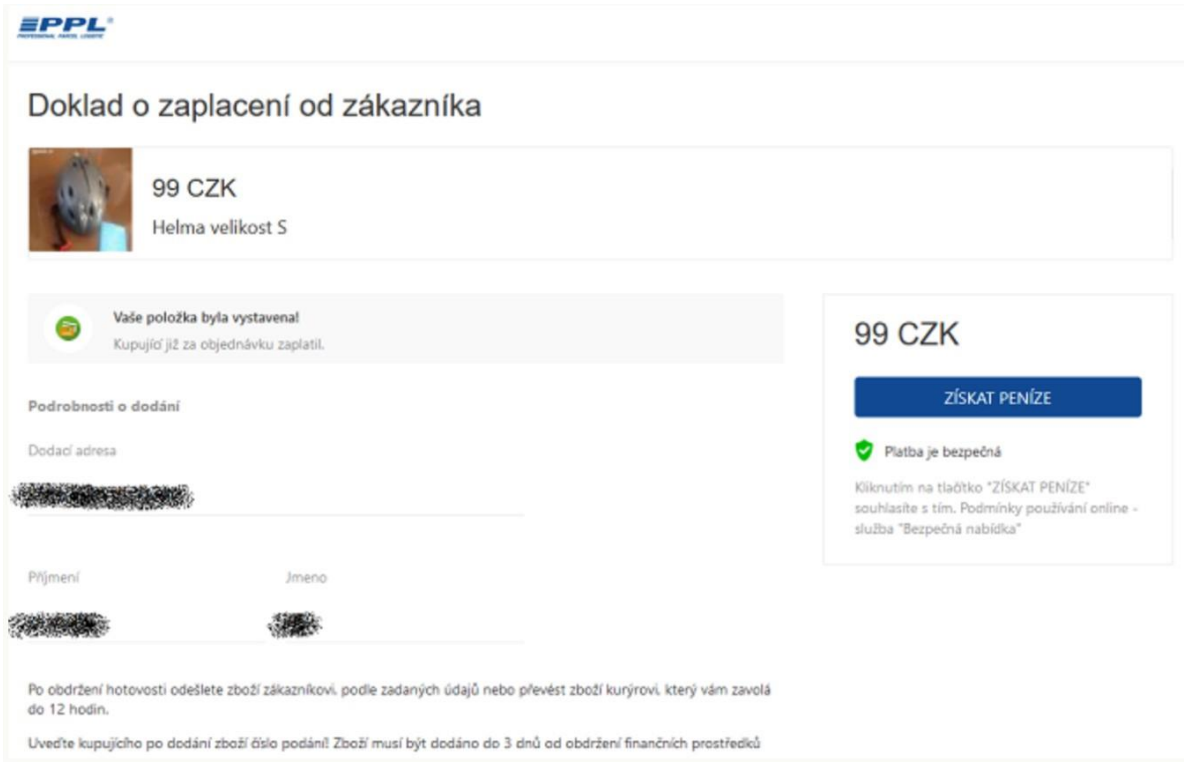
V posledních letech se v České republice rozšířil podvod na online bazarech, tzv. phishing. „*Phishing je forma útoku s pomocí technik sociálního inženýrství, kdy se útočník vydává za důvěryhodnou autoritu s cílem získat citlivá data oběti*.“ (Eset, 2022). V tomto širším slova smyslu je phishing spojen s podvodným jednáním, které je založeno na povzbuzení důvěry oběti, snížení její odstražitosti. Cílem phishingu je vždy získat citlivé informace oběti, které mohou být vyžadovány přímo (např. vyplněním formuláře) nebo odcizeny prostřednictvím malware, který si citlivé údaje posbírá sám (Kolouch, 2003).

V návaznosti na stále rostoucí počet případů podvodů tohoto typů při obchodování s použitým zbožím vydala Policie České republiky varovné upozornění (Hrdina, 2022). Jedná se o situace, kdy podvodník předstírá, že se zajímá o nákup zboží, prodávaného soukromou osobou na online bazarech (např. Marketplace na Facebooku, Aukro, Bazoš, Sbazar.cz). Podvodník zpravidla kontaktuje prodejce prostřednictvím online Messengeru a projevuje zájem o zboží. Může položit otázky, které zvyšují důvěru prodejce v to, že je to skutečný zájemce o nákup – např. „Je tento inzerát ještě aktuální?“. Pak obvykle říká prodejci, že je v zahraničí nebo „je velice zaneprázdněn“. Kvůli tomu žádá prodejce, aby poslal mu zboží přes kurýrní službu – PPL, DPD, Českou poštu atd. Existují různé varianty uhrazení nákupu, které podvodníci uvádějí, platba na dobírku, platba online kartou, platba

kurýru atd. Dále žádají prodejce, aby jim sdělil osobní informace, které jako by potřebují k objednání kurýrní služby. Velmi často posílají prodejci odkaz, kde musí prodejce vyplnit své údaje, včetně údajů o platební kartě. Po rozkliknutí odkazu se prodejci zobrazí stránka, která velmi dobře kopíruje stránky známých kurýrních společností – ppl.cz, dpd.cz. Pokud jedinec bude věřit, že je to skutečná stránka kurýrní společností, údaje vyplní a budou tak odcizený podvodníkem.

Další variantou podvodu je, kdy se stránka dokonce zobrazuje fotografii zboží na prodej či možný chat. Podvodník uvádí, že se již objednal doručení zboží a provedl platbu. Prodejci nabízí možnost získat peníze přes odkaz (viz Obrázek 7). Tady se však skrývá podvod, protože pro získání peněz je třeba zadat údaje své platební karty, a to včetně CVV kódu, který umožňuje zločinci zneužívat debetní nebo kreditní kartu oběti.

Obrázek 7: Ilustrační příklad podvodu na online bazarech v ČR – falešné potvrzení o zaplacení zboží



Zdroj: Zendulka, 2022

3.4.4 Způsoby, jak podvodníci mohou obejít dvoufaktorovou identifikace

Je třeba dodat, že kvůli dvoufaktorové identifikaci nestačí k provedení platby pouze znát CVV kód, ale je potřeba provést například potvrzení v online bankovnictví. Stále však existují způsoby, jak údaje platební karty využit i bez dvoufaktorového potvrzení a podvodníci tyto cesty znají (Zendulka, 2022).

Jedním ze způsobů je vypátrání, tedy odcizením jednorázových kódů v SMS, zasílaných na telefon uživatele v rámci dvoufaktorové identifikace. Podvodník nejprve zašle uživateli zprávu, která vypadá jako zpráva od banky a bude obsahovat odkaz na webovou stránku, která vypadá také velmi podobně jako web banky. Doména podvodné stránky může se nepatrně lišit od originální adresy banky. Zaznamenat rozdíl je zejména obtížné, pokud je odkaz otevřen v mobilním zařízení, kde se zobrazuje pouze začátek URL adresy a její zbytek je skrytý. Podvodná stránka může obsahovat i SSL zabezpečení (URL má na začátku https://) a díky zobrazovanému zámku zvyšovat pocit bezpečnosti u uživatelů. Riziko je vysoké zejména proto, že málokdo bude číst detaily SSL certifikátu (Lohnert, 2021).

Pokud uživatel bude věřit, že je na originální stránce své banky, zadá tam své přihlašovací jméno a heslo. V tomto kroku získá podvodník první klíč pro vstup. V reálném čase podvodník ručně zadá tyto údaje do skutečného webového rozhrání banky. V tomto okamžiku pošle banka autentifikační SMS kód. Oběť zadá tento kód do falešné stránky a podvodník opět ho uvidí a použije k úspěšné dvoufaktorové identifikaci. Podvodník může vstoupit i do skutečného rozhrání internetového bankovnictví uživatele. V době, kdy se uživatel stále nachází na falešné stránce, bude mu zobrazeno upozornění, že se přihlášení stále trvá. V této době podvodník zadá příkaz k platbě v internetovém bankovnictví. K potvrzení bude opět požadovat kód. Na falešné stránce se uživateli zobrazí hlášení, že se něco pokazilo a že musí zadat nový SMS kód. Druhý kód, který mu byl skutečně odeslán (ale pro účely podvodného příkazu k úhradě), předá podvodníkovi přes falešnou stránku, který ho úspěšně použije pro krádež peněz z účtu oběti (Lohnert, 2021).

3.4.5 Phishing – telefonní volání od banky nebo policie

Další varianta phishingu v ČR je založena na principu telefonních hovorů, kdy se podvodník představí jako pracovník banky nebo policie. Oběti může být například sdělena informace, že jeho účet byl napaden hackeři a kvůli tomu je žádoucí, aby prostředky byly převedeny na jiný účet. Věrohodnost pokynů může být zvýšena tím, že po jednom volání od

fiktivního bankovního pracovníka, zavolá fiktivní policista, který potvrdí správnost informací, uvedených bankovním pracovníkem (Policie ČR, 2021).

Ke zvýšení důvěry oběti mohou volající využit také metodu tzv. spoofingu telefonního čísla, která dokáže napodobit jakékoliv telefonní číslo, infolinku bankovní instituce atd. (Policie ČR, 2021).

Oběť je zpravidla požádána, aby poskytla své osobní informace volajícímu. Následně může oběť získat e-mail s odkazem na stránku, kde bude poskytnut možnost převést peníze na nový jakoby „bezpečný“ a dočasný účet.

3.5 Způsoby ochrany proti podvodům s platebními kartami

Povaha a rozsah podvodů s platebními kartami jsou dynamické a vyžadují neustálý vývoj nových řešení a také větší spolupráci napříč všemi články platebního řetězce. Vznikající hrozby podvodů a řešení potřebná k jejich zmírnění jsou technicky stále složitější.

- **Nelze sdílet osobní data třetím osobám**

Moderní platební karty jsou vybavena základními ochrannými prvky, jako jsou identifikační údaje uživatele, CVV kód a PIN (Personal Identification Number). Je zřejmé, že pro bezpečnost by neměla tato data být sdělena třetím osobám. Nelze platební údaje sdělovat volajícím na telefon ani přes e-mail nebo Messengery. Při zadávání PIN kódu je vhodné zakrývat klávesnici nebo displej bankomatu od nežádoucích diváků.

- **Nelze opouštět bankomat při zaseknutí karty**

Když se karta, vložená do bankomatu, nevysune zpět, nelze opouštět bankomat (Kapitol, 2016). Je to rozšířený postup, kdy zločinec používá zařízení pro zaseknutí karty a má prostředky k tomu, aby tuto kartu samostatně vyzvednul. Tímto případům se bankovní instituce brání tím, že instalují kamerová zařízení v místě instalace bankomatu. Je však třeba mít na paměti, že je lépe krádeži karty předejít než pak hledat zločince podle záznamu z kamer. Není také známo, jak rychle dokáže zločinec kartu použit a jak rychle jedinec přijde o své prostředky na kartě.

- **Nastavení limitů pro platby kartou**

Jednoduchým opatřením, jak následky krádeže karty zmírnit, je nastavit limity pro výběr hotovosti v bankomatech, platby kartou v obchodech a na internetu. Limit je vhodné nastavit na co nejnižší přijatelnou úroveň. Pokud ke krádeži došlo, je také okamžitě incident nahlásit bance a kartu zablokovat.

- **Nálepka na magnetický proužek na kartě**

Pro ochranu dat na magnetickém proužku platební karty, která jsou zranitelná před různými skimmingovými techniky, byly vyvinuty speciální nálepky. Jde o bezpečnostní známky, které se lepí na magnetický proužek, a které braní čtení dat z magnetického proužku. Například, pokud je v bankomatu naistalováno skimmingové zařízení, zacílené na magnetický proužek, známka způsobí to, že karta bude uživateli vrácena zpět bez možnosti provést operaci. Známka má však nevýhodu, která spočívá v možnosti využívat kartu pouze v bankomatech, které mají nastavenou prioritu čtení dat na čip. Nalepená bezpečnostní známka tedy brání čtení dat z magnetického proužku jak podvodníkům, tak i bance, pokud její bankomat využívá magnetický proužek jako zdroj potřebných dat (CZ Protect, 2022). Nálepky nejsou dnes proto příliš používány, a také zejména kvůli technologickému pokroku a využití čipů ve všech moderních platebních kartách.

- **Čipové platební karty a bezkontaktní platby**

Čip na platební kartě je velmi silný bezpečnostní prvek a načíst z něho data je pro podvodníky velmi obtížně. V dubnu 2011 se objevily zprávy, že vědci ve Velké Británii dokázaly načíst data z čipu. Jejich způsob nelze však považovat za významný průlom, který by využili podvodníci. Vědci odbrousili některé vrstvy odcizené platební karty a pod mikroskopem nainstalovali několik drátků na přesně určené plošky čipu. Drátky se spojili s počítačem, který nasimuluje zadání správného PINu (CZ Protect, 2022).

Využití systému bezkontaktních plateb snížil riziko odcizení karet a krádeže údajů karty. Pro zákazníky je proto vhodné používat bezkontaktní platbu všude, kde je to možné, aniž by vkládaly kartu do terminálu nebo bankomatu.

- **Pojištění proti ztrátě a krádeži**

Pojištění proti ztrátě a krádeži platební karty je účinným způsobem, který ochrání uživatele před ztrátou svých prostředků z důvodu jednání zločinců. Pojištění je zejména žádoucí při cestování do zahraničí, kdy jedinec nemá fyzicky přístup ke svým jiným platebním kartám, hotovosti nebo nemá možnost navštívit pobočku banky a čekat na vydání nové platební karty.

V posledních letech se objevil nový produkt na bankovním trhu – pojištění internetových rizik. Například ČSOB nabízí tento typ pojištění pro majitele platebních karet všech bank v ČR. Pojištění zahrnuje například řešení reklamace na poškozený nebo jiný výrobek, nakoupený online v ČR nebo v zahraničí, podporu v případě zneužití identity (využití internetového bankovnictví nebo sjednání půjčky cizí osobou), podporu v případě zneužití karty při platbě na internetu, IT asistenci (ČSOB, 2022).

- **Pravidelná kontrola pohybů na účtu**

Pravidelná kontrola výdajů v osobním bankovnictví pomáhá včas identifikovat zneužití karty. Některé banky (například ČSOB) automaticky sledují pohyby na účtech svých klientů a v případě výskytu neobvyklých transakcí (např. do jiných vzdálených zemí, na mnoha osobních účtů cizinců s malými nebo naopak velkými částkami) kontaktují majitele účtu s prosbou to zkontrolovat.

- **Kontrola důvěryhodnosti prodejce a webových stránek**

Při platbě kartou online je důležité dávat pozor na důvěryhodnost prodejce a jeho webové stránky. Zejména obezřetný musí být spotřebitel při využití služeb nového a neznámého obchodníku. Zákazník by měl upřednostňovat e-shopy s využitím vysokého standardu zabezpečení 3D Secure, kdy je potřeba potvrzovat platbu pomoci aplikace bankovnictví v mobilním telefonu nebo pomoci speciálního kódu, zasílaného na telefon (ČSOB, 2023). Je zde třeba mít na paměti, že existují různé fishingové techniky a podvodníci jsou schopni kopírovat jakékoliv telefonní čísla, e-mailové adresy a nabodovat webové stránky důvěryhodných institucí.

- **Bezpečností opatření pro maloobchodníky**

Pro maloobchodníky jsou k dispozici různé softwarové technologie, určené k detekci podvodů s platebními kartami – např. Fraud Protection od společnosti Microsoft. Využití ochranného software pomáhá nejen předejít rizikům, která jsou spojená s podvody, ale i zlepšit vnímání jejich značky zákazníky. „*Podle zprávy organizace Experian 2020 Global Identity and Fraud Report o identitě a podvodech téměř 90 procent zákazníků tvrdí, že se jejich vnímání firmy zlepšuje, když společnost investuje do zlepšení zákaznického prostředí, a to včetně zabezpečení.*“ (Microsoft, 2022).

Dále jsou pro maloobchodníky relevantní následující ochranná opatření (Microsoft, 2022):

- pravidelná aktualizace systému pro nákupy platební kartou, využití moderních systémů POS a CRM,
- splnění standardů pro zabezpečení platebních karet PCI DSS (Payment Card Industry Data Security Standard), který zvyšuje ochranu informací o platebních kartách klientů,
- využití nástrojů, které identifkují varovné signály – např. odlišné fakturační a dodací adresy, více objednávek od jednoho zákazníka s využitím více karet, více hromadných objednávek uhrazených stejnou kartou, náhlý růst objemu objednávek klienta atd.,
- zvážit možnost využití dalších platforem, jako např. služba ověření adresy, která potvrdí fakturační adresu držitele karty u vydavatele karty.

4 Vlastní práce

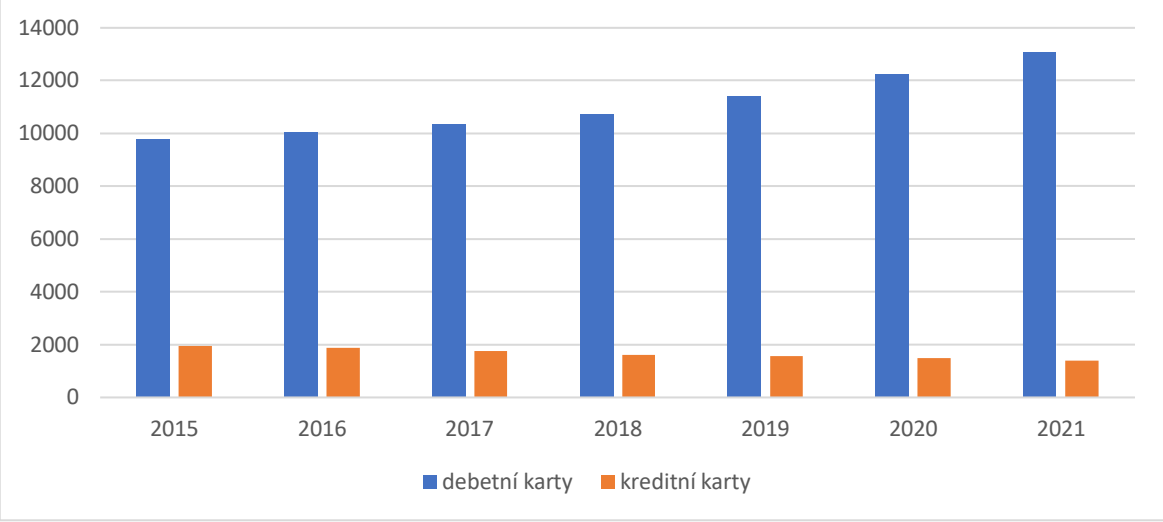
4.1 Využití platebních karet v ČR

Platební karty se stály velmi populárním způsobem placení v České republice, což dokládají statistiky České národní banky, výzkumy Češi a platební styk, data Českého statistické úřadu a mnoho menších studií, provedených různými organizacemi, výzkumníky a medií. Není možné v rámci omezeného rozsahu této práce popsat výsledky všech těchto výzkumů. Dále je proto vytvořen základní přehled o využití platebních karet v ČR na základě dat z nejrozsáhlejších statistických průzkumů, které publikuje a komentuje například Česká národní banka.

4.1.1 Počty karet a přijímacích zařízení

Celkový počet platebních karet (bez ohledu na počet jejich funkcí) i počet platebních terminálů dlouhodobě zaznamenávají v České republice růst. V roce 2021 se dle údajů ČNB (2023) celkový počet karet vydaných českými bankami a pobočkami zahraničních bank působícími v ČR se meziročně zvýšil o 702 tisíce a na konci roku 2021 dosáhl 14,5 milionu karet. Z tohoto počtu bylo 13,1 milionu debetních karet (90,3 %). Počet kreditních karet na rozdíl od debetních karet však dlouhodobě meziročně klesá: v roce 2021 se jednalo o meziroční pokles 95 tisíc karet; celkový počet kreditních karet činil 1,4 milionu v roce 2021. Vývoj počtu debetních a kreditních karet je znázorněn pomoci grafu 1.

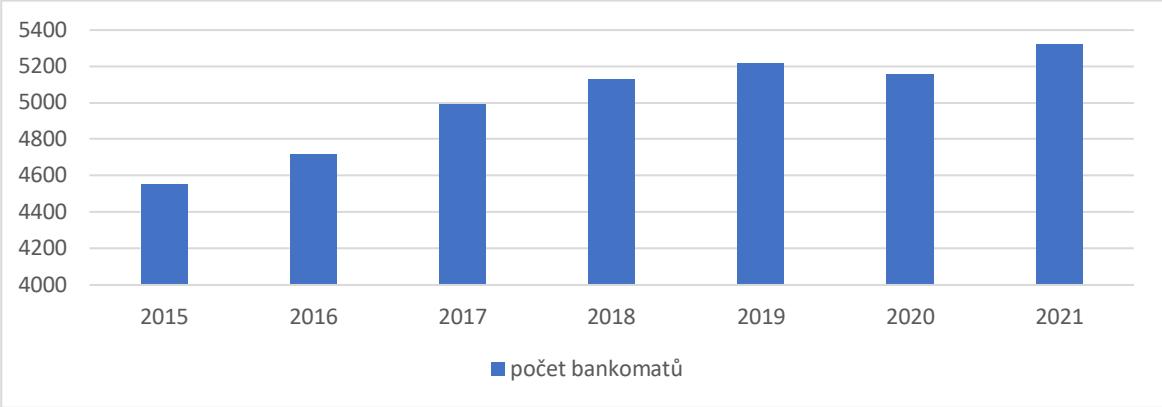
Graf 1: Počet debetních a kreditních karet v ČR (údaje ke konci roku; počet v tis.)



Zdroj: vlastní zpracování, ČNB (2023)

Počet bankomatů provozovaných českými bankami vzrostl o 164 na 5300 zařízení v roce 2021. Z tohoto celkového počtu bankomatů bylo 95 % bankomatů s funkcí výběru hotovosti (5 051 bankomatů v roce 2021). Tyto údaje nezahrnují instituce, které nemají oprávnění k poskytování platebních služeb a provozují bankomaty v České republice (Je to proto, že provoz bankomatu jako takový není platební službou). Vývoj počtu bankomatů v období 2015-2021 je ilustrován pomoci grafu 2.

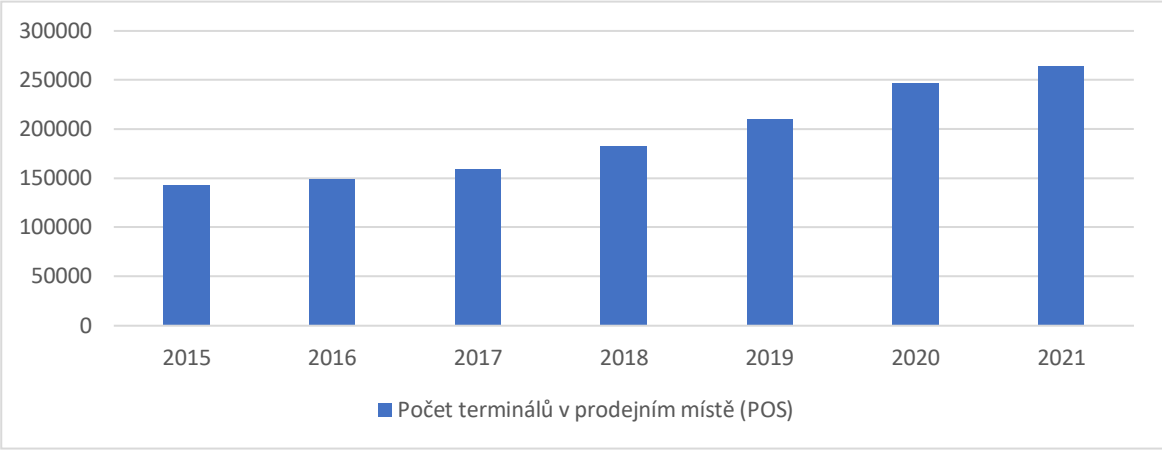
Graf 2: Počet bankomatů v ČR (údaje ke konci roku)



Zdroj: vlastní zpracování, ČNB (2023)

Počet terminálů v místě prodeje (POS) vydaných českým akvizitorem meziročně vzrostl o 18 tisíc na 264 tisíc zařízení na konci roku 2021. Tyto údaje však zahrnují i provozované bankomaty. Vývoj počtu POS terminálů v období 2015-2021 je znázorněn pomoci grafu 3.

Graf 3: Počet terminálů v prodejním místě (POS) v ČR (údaje ke konci roku)



Zdroj: vlastní zpracování, ČNB (2023)

Z výsledků analýzy základních statistik ČNB lze udělat závěr, že počet platebních karet, vydaných v ČR (14,5 mil. karet bez ohledu na počet jejich funkcí) značně převyšuje počet obyvatel v zemi (10,5 mil. osob). Je zřejmé, že část lidí vlastní více než 1 kartu na osobu. Trend růstu počtu platebních karet, počtu bankomatů a POS terminálů naznačuje význam využití platebních karet při účely placení v offline a online obchodech, operace s hotovostí (výběr a vklad). Naležitá ochrana v těchto oblastech je podmínkou bezpečností platebních prostředků obyvatel ČR.

4.1.2 Češi a platební styk

Každoroční průzkumy České bankovní asociace (ČBA) „Češi a platební styk" jsou cenným zdrojem informací o vzorcích chování a preferencích obyvatel při placení jejich nákupů. Následující charakteristika výstižně popisuje přístup českých obyvatel k platebními styku: „*Češi jsou tradičním i moderním národem zároveň. Na jedné straně jsou otevřeni inovacím, na straně druhé se odmítají vzdát již tradičních způsobů placení.*" (ČBA, 2021). Vzhledem k tomuto trendu je hotovost stále široce používaným platebním prostředkem v ČR. Zároveň se rozšiřují možnosti placení bezhotovostně a bezkontaktně, s využitím různých moderních technologií (např. hodinky, mobil, nálepky). Velký počet a různorodost možností placení lze považovat jako faktor určité svobody, která je pro české obyvatelstvo vysoce cenná.

Klíčová zjištění z posledního průzkumu ČBA (2021) jsou následující:

- 69 % Čechů používá debetní platební karty, 55 % - platí i v hotovosti,
- mírný pokles je dlouhodobě pozorován u využití kreditních karet (17 % v roce 2021),
- růst populárnosti placení přiložením mobilního telefonu (17 % v roce 2021),
- na internetu se nejčastěji platí kartou přes platební bránu (58 %).

Je zřejmé, že platební karty jsou součástí nejpopulárnějších způsobů placení v ČR. Je to další faktor, který naznačuje aktuálnost tématu bezpečnosti karet.

4.2 Dotazníkové šetření

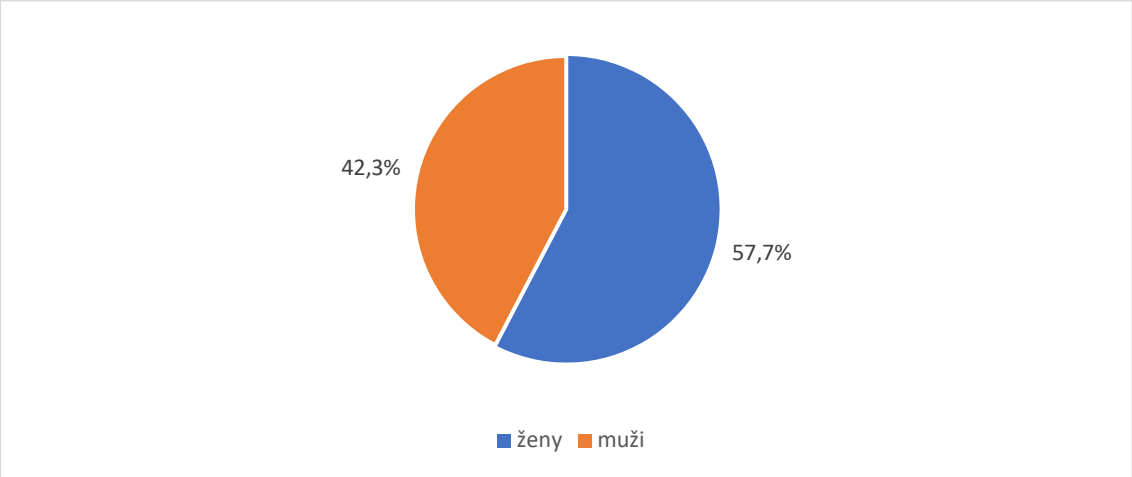
Cílem provedeného šetření je zhodnotit povědomí dotazovaných obyvatel ČR o podvodech, spojených s využitím PK, a možnostech ochrany proti nim. K analýze jsou použito celkem 137 vyplněných dotazníků. Formulář dotazníku je uveden v příloze A. Na začátku dotazníku jsou potenciální respondenty informováni o potřebě splňovat následující podmínky pro účast v průzkumu:

- respondent v současné době bydlí v ČR,
- respondent využívá platební karty pro své nákupy.

4.2.1 Základní charakteristika respondentů

Dotazník byl vyplněn 79 ženy (57,7 % na celkovém počtu respondentů) a 58 muži (42,3 %). Struktura respondentů dle pohlaví je znázorněna pomoci grafu 4.

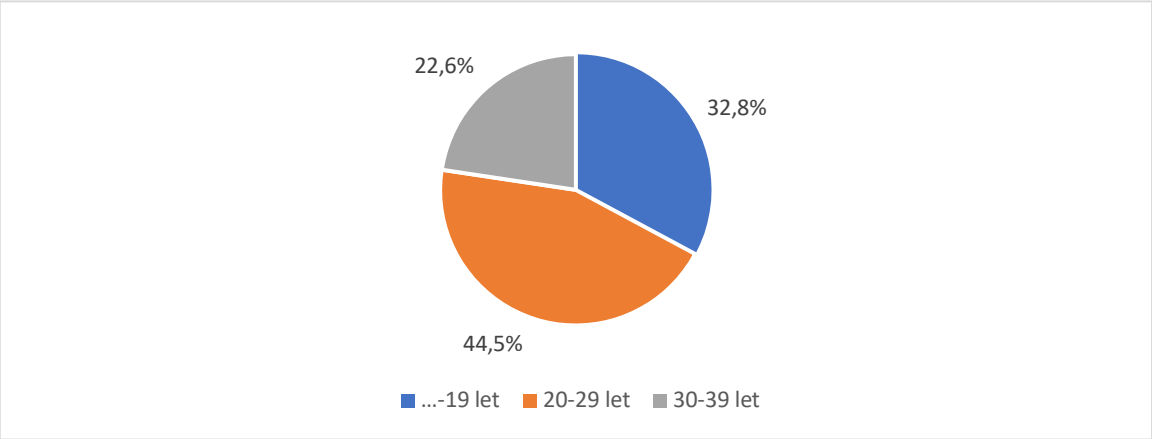
Graf 4: Pohlaví respondentů



Zdroj: vlastní zpracování, 2023

Z hlediska věkové struktury (graf 5) vytváří největší skupinu respondenti ve věku od 20 do 29 let (celkem 61 osob, 44,5 %). Třetina respondentů je mladších ve věku 19 nebo méně let (45 osob, 32,8 %). Ostatní respondenti (31 osob, 22,6 %) jsou ve věku 30-39 let. Lze tvrdit, že účastníci průzkumu jsou především ladí lidé a lidé středního věku, maximálně do 39 let.

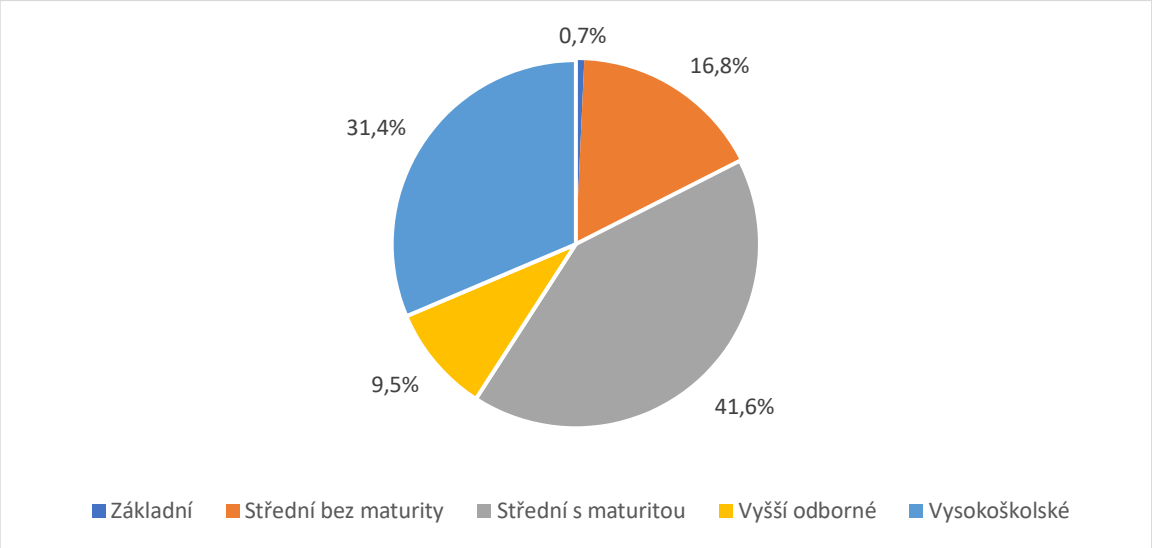
Graf 5: Věk respondentů



Zdroj: vlastní zpracování, 2023

Větší část respondentů má středoškolské vzdělání s maturitou (57 osob, 41,6 %). Téměř třetina respondentů (43 osoby, 31,4 %) má vysokoškolské vzdělání (graf 6).

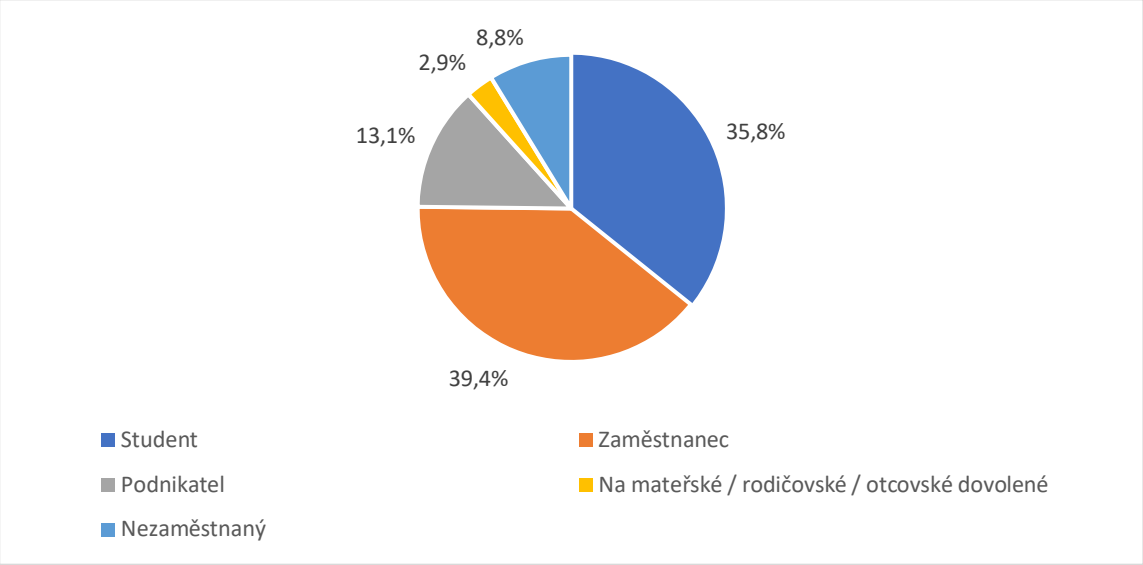
Graf 6: Nejvyšší dosažené vzdělání respondentů



Zdroj: vlastní zpracování, 2023

Přehled struktury respondentů dle jejich hlavní činnosti je vytvořen prostřednictvím grafu 7. 54 respondentů (39,4 %) jsou zaměstnanci, 49 osob (35,8 %) – student. Jsou to největší skupiny ve struktuře respondentů.

Graf 7: Hlavní činnost respondentů



Zdroj: vlastní zpracování, 2023

Je třeba upozornit, že dále uvedené názory a odpovědi se týkají pouze dotazovaných osob a nelze je zobecnit na celou populaci ČR. Na průzkumu se nejvíce podíleli mladí lidé ve věku do 29 let, studenti a zaměstnanci, mající vysokoškolské nebo středoškolské vzdělání s maturitou. Podíl mužů a žen je mezi respondenty přibližně stejný.

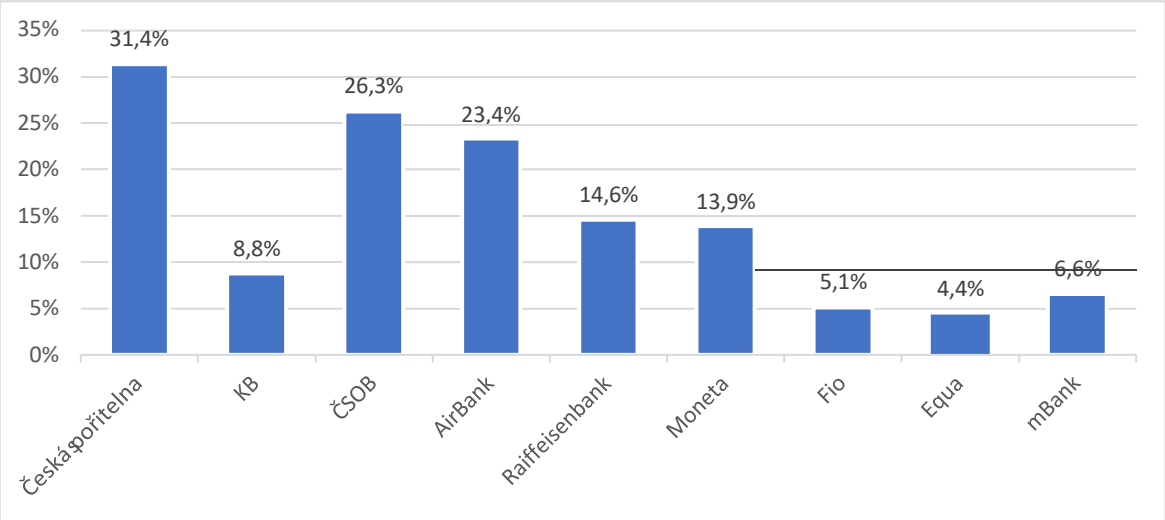
4.2.2 Způsoby využití platebních karet

V této části dotazníku bylo zjištěno, jak respondenti obvykle používají své platební karty – jak často, pro jaké účely apod. Je také zjištěno, jaký význam respondenti přisuzují bezhotovostním a hotovostním platbám všeobecně. Na základě toho lze udělat závěr o tom, jak důležité je bezpečné využití karet pro respondenty.

Otázka č. 1: Platební kartu jaké banky využíváte v současné době? (pokud používáte více platebních karet, uveďte max. 3 banky, které využíváte nejvíce)

Celkem 90 osob (65,7 %) uvedlo, že používá pouze platební kartu u jedné banky. 41 osob (29,9 %) uvedlo, že používá karty od 2 bank, 6 osob (4,4 %) – od 3 bank. Nejvíce respondentů jsou klienty České spořitelny (43 osoby, 31,3 %) – viz graf 5. Další populární banky mezi respondenty jsou ČSOB (36 osob, 26,3 %), AirBank (32 osoby, 23,4 %). Dále dle populárnosti následují Raiffeisenbank (20 osob, 14,6 %) a Moneta (19 osob, 13,9 %). Méně populární jsou mezi respondenty banky Fio, Equa, mBank a KB.

Graf 8: Platební kartu jaké banky využíváte v současné době?



Zdroj: vlastní zpracování, 2023

Otázka č. 2: Jak často využíváte uvedené způsoby placení?

Přehled odpovědí o frekvenci využití různých způsobů placení je uveden v tabulce 1.

Tabulka 1: Jak často využíváte uvedené způsoby placení?

	Nikdy	1x za půlroku / vzácněji	Cca 1x měsíčně	Cca 1x týdně	Několi krát týdně	Denně	Nevím
Hotovost	0	0	28	32	54	13	10
	0,0 %	0,0 %	20,4 %	23,4 %	39,4 %	9,5 %	7,3 %
Debetní platební karta	0	0	2	5	24	104	2
	0,0 %	0,0 %	1,5 %	3,6 %	17,5 %	75,9 %	1,5 %
Kreditní karta	43	28	19	2	8	28	9
	31,4 %	20,4 %	13,9 %	1,5 %	5,8 %	20,4 %	6,6 %
Mobilní telefon (Apple Pay, Google Pay…)	46	4	2	8	16	54	7
	33,6 %	2,9 %	1,5 %	5,8 %	11,7 %	39,4 %	5,1 %
Chytré hodinky	102	3	2	0	13	12	5
	74,5 %	2,2 %	1,5 %	0,0 %	9,5 %	8,8 %	3,6 %
Platební „známka“ na mobilu, klíčích…	97	2	0	5	8	5	20
	70,8 %	1,5 %	0,0 %	3,6 %	5,8 %	3,6 %	14,6 %

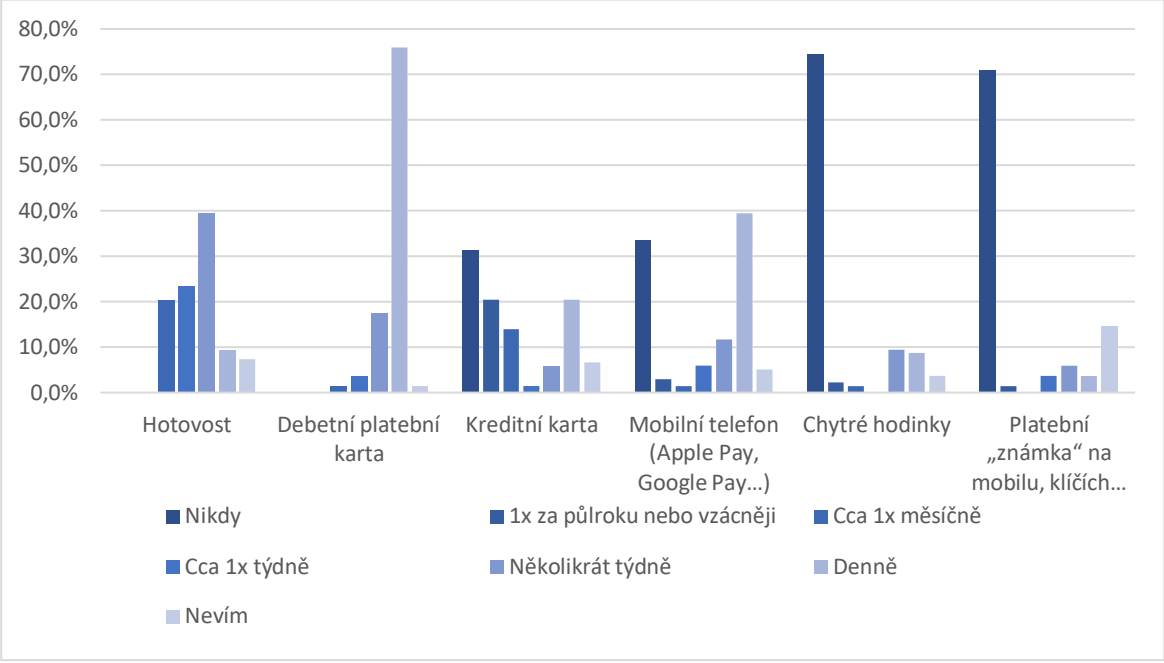
Zdroj: vlastní zpracování, 2023

Na základě výše uvedených odpovědí je nakreslen graf. Debetní platební karty jsou významným konkurentem hotovosti – denně jsou využívány 75,9 % respondentů (104 osob). Hotovost je využívána k placení velkým počtem respondentů, ale frekvence je nižší – obvykle se používá několikrát týdně (39,4 % respondentů) až cca jednou za týden (23,4 %) nebo jednou za měsíc (20,4 %). Vzhledem k vyšší frekvenci využití platebních karet oproti využití hotovosti lze tvrdit, že bezpečnost bezhotovostních plateb je pro respondenty zásadní otázkou.

Frekvence využití ostatních druhů platebních prostředků je nižší než u platebních karet a hotovosti. Lídrem jsou zde mobilní telefony a kreditní karty. Zatím významně zaostávají za nimi chytré hodinky, které zatím využívány jen cca pětinou respondentů. Platební známky jsou méně využíváním i méně známým způsobem placení. Na základě těchto výsledků lze se domnívat, že bezpečnost moderních bezkontaktních způsobů placení, jako jsou mobilní zařízení a hodinky, je také pro respondenty důležitá.

Přehled odpovědí o frekvenci využití různých druhů placení je znázorněn pomoci grafu 9.

Graf 9: Jak často využíváte uvedené způsoby placení?

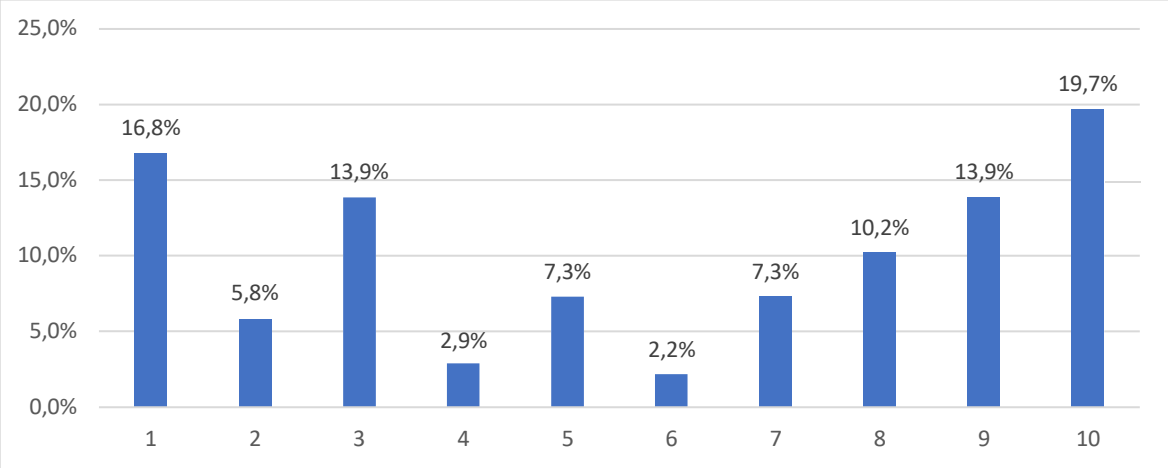


Zdroj: vlastní zpracování, 2023

Otázka č. 3: Co si myslíte o tom, kdyby přestala existovat hotovost? Pro odpovědi použijte 10bodobou škálu, kde 1 = „Rozhodně bych to neuvítal(a); je to omezení svobody“, 5 =„Půl na půl“, 10 =„Uvítal(a) bych to; je to zjednodušení života“.

Tato otázka také umožnila vyhodnotit význam bezhotovostního platebního styku pro respondenty. Výsledky jsou znázorněny pomoci grafu 10. Je patrné, že je zde významný rozptyl v odpovědích – mnoho respondentů je výrazně proti omezení využití hotovosti, a o něco vyšší počet respondentů by zásadně uvítal odstranění hotovosti z platebního styku. Názory na tuto otázku nejsou zatím jednotné, proto význam hotovosti je stále pro mnoho respondentů vysoký. Bezpečnost platebních karet je proto pro tuto část respondentů méně významná, protože mohou platby karty snadně nahradit placením v hotovosti.

Graf 10: Co si myslíte o tom, kdyby přestala existovat hotovost? (10bodová škála*)



***Poznámka k použité **škále**: 1 = „Rozhodně bych to neuvítal(a); je to omezení svobody“, 5 =„Půl na půl“, 10 =„Uvítal(a) bych to; je to zjednodušení života“.

Zdroj: vlastní zpracování, 2023

Otázka č. 4: Při výběru hotovosti z bankomatu, jaký z uvedených způsobů používáte (za předpokladu, že máte k dispozici obě možnosti)?

Banky upozorňuji své klienty na výhody placení bezkontaktně. Platí to i pro využití bankomatů – ty, které jsou označeny symbolem bezkontaktní platby, umožňují jednoduché přiložení karty. Vložení karty přímo do bankomatu je spojeno s rizikem, že dojde k chybě a bankomat kartu zadrží, nebo s podvodem, v případě že na bankomat bylo nainstalováno skimmingové zařízení. V České republice jsou Policií zapátrány případy, kdy byly v bankomatech nainstalována tato zařízení, proto je zde riziko podvodu. V zahraničí,

zejména v méně rozvinutých zemích, je pravděpodobnost potkat se se skimmingovým zařízením vyšší. Je třeba proto této oblasti bezpečnosti věnovat zvláštní pozornost.

Většina respondentů uvedla, že preferuje bezkontaktní využití bankomatů, pokud mají tuto možnost k dispozici, což je pozitivní zjištění.

Graf 11: Při výběru hotovosti z bankomatu, jaký z uvedených způsobů používáte (za předpokladu, že máte k dispozici obě možnosti)?

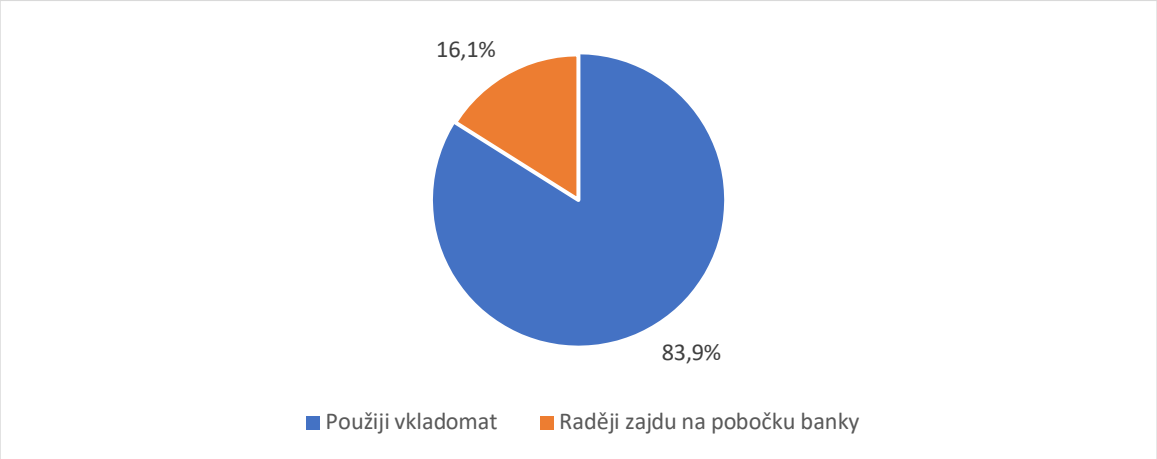
Zdroj: vlastní zpracování, 2023

Otázka č. 5: Pokud potřebujete vložit hotovost na účet a máte k dispozici obě dále uvedené možnosti, jaký způsob preferujete?

Využití pobočky banky pro vkládání hotovosti na účet je v některých případech bezpečnější než využití vkladomatu kvůli rizikům, že na vkladomatu je naistalováno podvodné zařízení. Osobní kontaktování personálu pobočky, poplatky spojené s využitím pokladny na pobočce, fronty – jsou to faktory, které mohou odradit klienta od návštěvy pobočky pro účely vložení peněz na svůj účet. Na místo toho raději využiti vkladomat, který umožní provést požadovanou operaci rychleji, pohodlněji a často i levněji.

115 respondentů (83,9 % osob) uvedli, že použiji vkladomat pro vkládání hotovosti, ostatní 22 dotazované osoby (16,1 %) mohou navštívit bankovní pobočku (viz graf níže). Znamená to, že vkladomaty jako způsob vkládání hotovosti jsou pozitivně přijímány respondenty. Naznačuje to potřebu zajistit bezpečnost vkladomatů, které využívají.

Graf 12: Pokud potřebujete vložit hotovost na účet a máte k dispozici obě dále uvedené možnosti, jaký způsob preferujete?



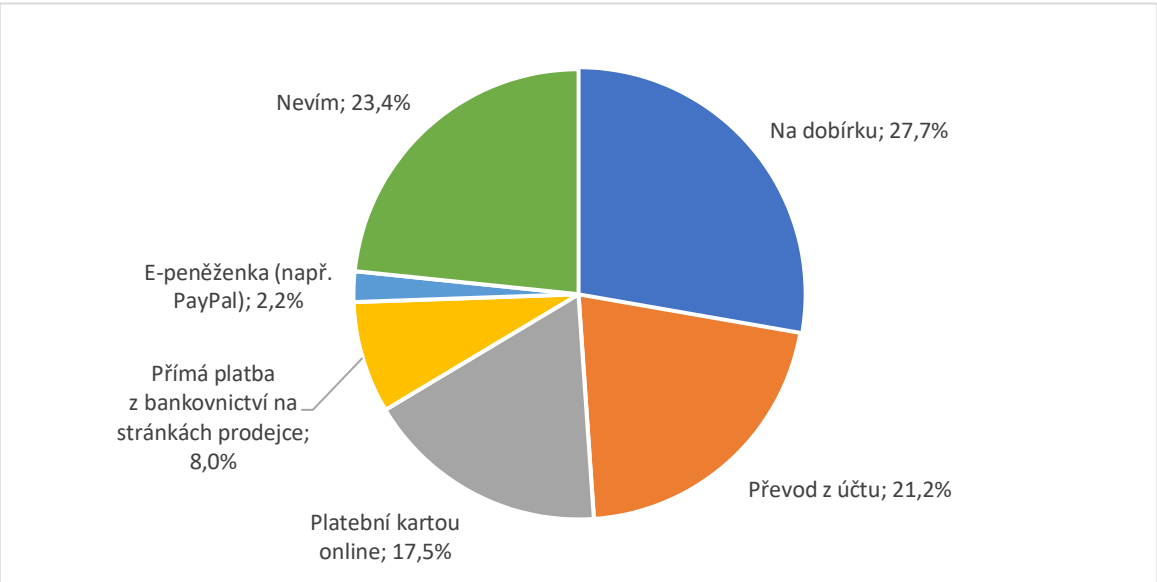
Zdroj: vlastní zpracování, 2023

4.2.3 Bezpečnost platebních karet

Otázka č. 6: Pokud u neznámého internetového prodejce nakupujete poprvé, jaký způsob placení s největší pravděpodobností zvolíte?

Struktura odpovědí respondentů ve vztahu k tomu, jaký typ placení preferují u neznámého online prodejce, je znázorněna pomoci grafu 13.

Graf 13: Pokud u neznámého internetového prodejce nakupujete poprvé, jaký způsob placení s největší pravděpodobností zvolíte?



Zdroj: vlastní zpracování, 2023

Při nákupu u neznámého e-shopu existuje riziko, že prodejce je podvodník nebo v nedostatečné míře chrání zájmy kupujícího. Pro tuto situaci je obvykle doporučeno si zvolit nejbezpečnější způsob platby – například na **dobírku**. 38 respondentů (27,7 %) uvedlo, že by si zvolilo právě tento typ placení u neznámého elektronického prodejce. Je zjištěno, že dobírka je více preferována ženy než muži: tuto variantu si zvolilo 28 žen (35,4 % všech dotazovaných žen v průzkumu) a 10 mužů (17,2 % všech mužů).

Převod z účtu je další relativně bezpečný způsob platby u neznámého prodejce. Platbu lze ve svém bankovnictví zrušit nebo vrátit. Informaci o platbě v bankovnictví lze také použit jako důkaz o zaplacení. Banky v současné době navíc často sledují platby na podezřelé účty podvodníků, proto upozorní klienta na riziko situace, kdy bude převádět peníze na účet, který patří mezi nespolehlivé. Převod z účtu je druhým populárním způsobem platby u neznámých prodejců mezi respondenty. Uvedli ho 29 osob (21,2 % všech respondentů). Je zjištěno, že tato odpověď byla více uvedena muži než ženy: 16 mužů (27,6 % všech dotazovaných mužů) a 13 žen (16,5 %).

Placení kartou online je méně bezpečným způsobem platby. Nicméně moderní opatření (jako například dvoufaktorová autentifikace) zvyšují bezpečnost plateb i u neznámých prodejců. Existují však případy, kdy podvodníci jsou schopni překonat bezpečnostní bariéry, což bylo zmíněno v teoretické části práce. Placení kartou by u neznámého prodejce použilo 24 respondentů, což představuje relativně velký podíl na celkovém počtu dotazovaných osob (17,5 %). Trochu více mužů než žen preferuje tento méně bezpečný způsob placení (11 žen neboli 13,9 %, 13 mužů neboli 22,4 %).

Přímá platba z bankovnictví na stránkách prodejce – je to méně bezpečná platba, protože je zde riziko krádeže dat pro přístup k účtu klienta. Tento způsob placení byl uveden menším počtem respondentů – 11 osob (8 %), z toho 6 žen (7,6 % všech žen v průzkumu) a 5 mužů (8,6 %).

E-peněženka (např. PayPal) je nejméně populární způsob platby vůbec – uvedlo ho pouze 3 osoby (2,2 %), proto není třeba tuto variantu nějakým způsobem komentovat.

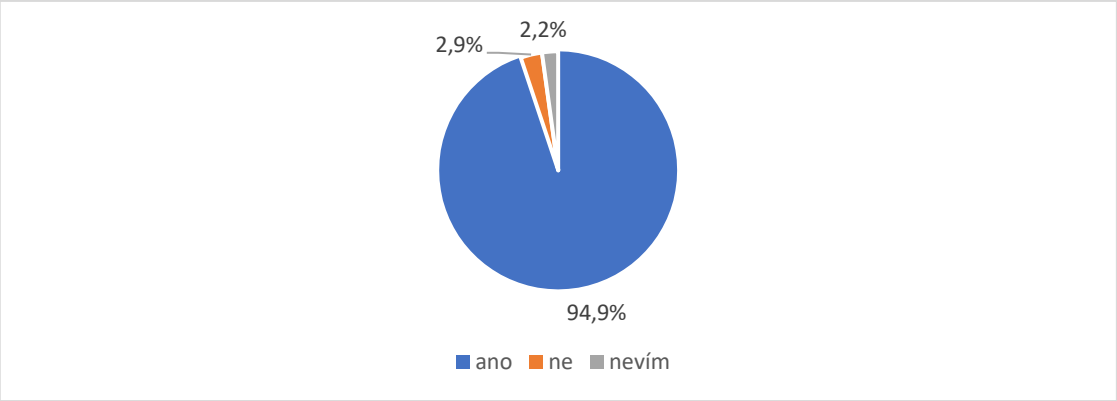
Odpověď **„nevím“** si zvolilo 32 respondentů (23,4 %), z toho 21 žena (26,6 % všech žen) a 11 mužů (19 %). Lze se domnívat, že respondenti budou rozhodovat o preferovaném

způsobu platby v závislosti na typu nákupu a po subjektivním zhodnocení spolehlivosti konkrétního prodejce. Je to také vhodná strategie při nákupu u neznámého prodejce.

Otázka č. 7: Máte nastavený limit pro platby kartou?

Nastavení limitu na platby kartou je jedním z jednoduchých a zároveň účinných způsobu zajištění bezpečnosti svých peněz na účtu v případě krádeže platební karty. Podvodník prostě nebude mít možnost použít tuto kartu k útratě větších částek. Přehled odpovědí respondentů na otázku o nastavení limitu na jejich kartách je uveden na grafu 14. Většina respondentů (130 osob, 94,9 %) konstatuje, že nastavený limit má, což je pozitivní zjištění.

Graf 14: Máte nastavený limit pro platby kartou?

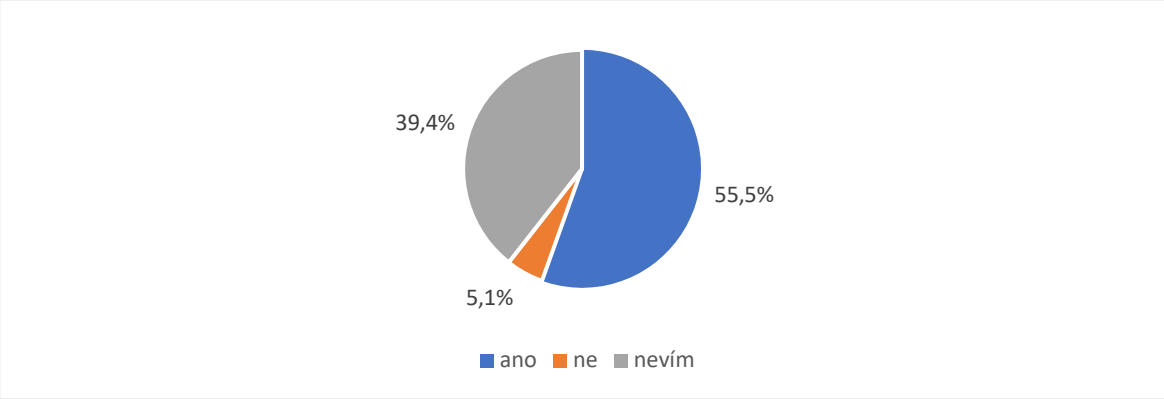


Zdroj: vlastní zpracování, 2023

Otázka č. 8: Máte platební kartu pojištěnou proti ztrátě a odcizení?

Pojištěné proti ztrátě a odcizení karty je další způsob zvýšit bezpečnost své platební karty, který poskytují finanční instituce. Povědomí o tomto způsobu ochrany platební karty je mezi respondenty relativně nižší. Nicméně více než polovina respondentů uvedla, že má tento typ pojištění (viz graf 15).

Graf 15: Máte platební kartu pojištěnou proti ztrátě a odcizení?



Zdroj: vlastní zpracování, 2023

Z podrobné analýzy odpovědí bylo zjištěno, že odpovědi „ne“ a „nevím“ byly nejčastěji uvedeny respondenty s nižší úrovni vzdělání. Čím vyšší je úroveň vzdělání respondentů, tím více uvádějí odpověď „ano“ a méně odpovědi „ne“ nebo „nevím“. Přehled odpovědí respondentů, rozdělených dle jejich nejvyšší úrovní vzdělání, je uveden v tabulce 2.

Tabulka 2: Máte platební kartu pojištěnou proti ztrátě a odcizení? – rozdělení odpovědí dle vzdělání respondentů

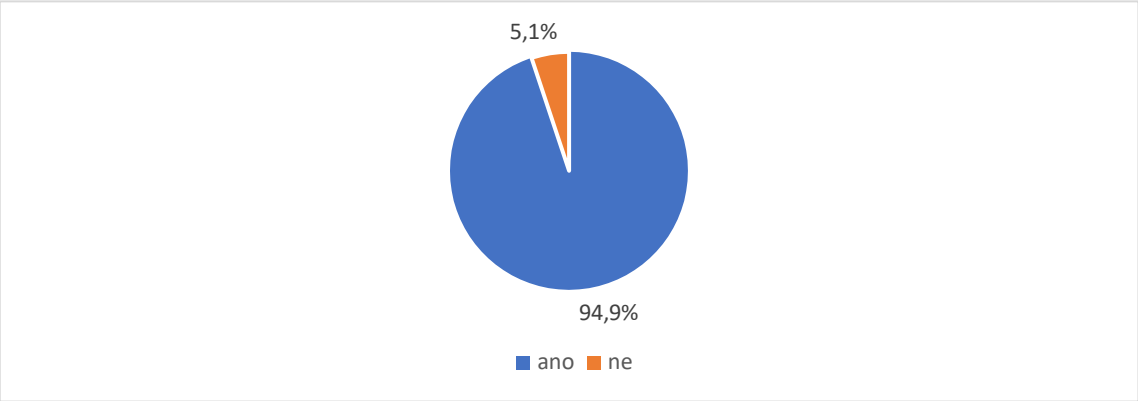
	Základní	SŠ bez maturity	SŠ s maturitou	Vyšší odborné	VŠ	Celkem
Ano	0	5	26	7	38	76
Ne	0	3	3	1	0	7
Nevím	1	15	28	5	5	54
Celkem	**1**	**23**	**57**	**13**	**43**	**137**

Zdroj: vlastní zpracování, 2023

Otázka č. 9: Pamatujete si svůj PIN kód k platební kartě?

Z hlediska bezpečnosti je lépe si PIN kód k platební karty pamatovat. V žádném případě není vhodné vypisovat kód přímo na platební kartu nebo na do peněženky. Vzhledem k velkému objemu informací a různých hesel, který musí člověk v dnešní době pamatovat, je možné, že si na svůj PIN zapomene. Nicméně z výsledků průzkumu vyplývá, že překvapivé velký podíl respondentů uvedlo, že si svůj PIN pamatuje (130 osob, 94,9 %) – viz graf 16.

Graf 16: Pamatujete si svůj PIN kód k platební kartě?



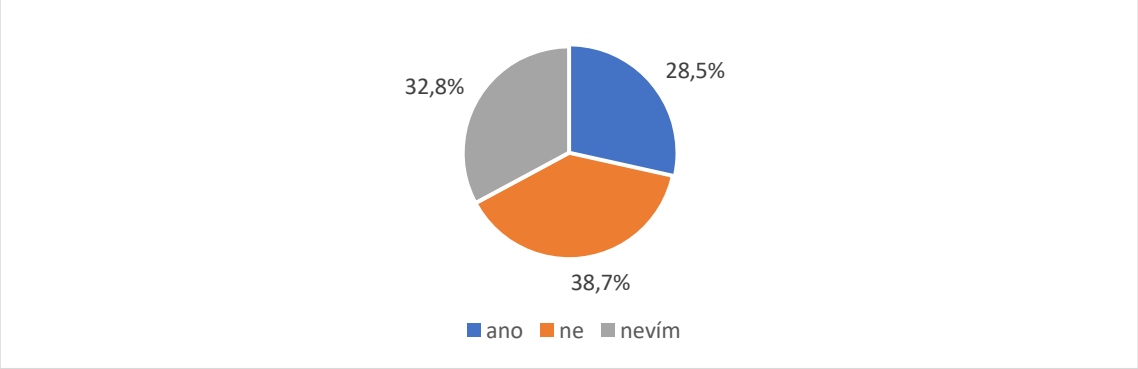
Zdroj: vlastní zpracování, 2023

Otázka č. 10: Používáte službu 3D Secure?

Využití služby 3D Secure zajišťuje vysoké standardy bezpečnosti, ale neposkytuje 100% ochranu, protože podvodníci někdy používají různé fishingové techniky. Nicméně jsou technicky náročnější a proto relativně vzácnější. Služeb 3D Secure je proto stále důelžitým prvkem bezpečnosti.

Z výsledků průzkumu však vyplývá nedostatečná znalost respondentů o této službě – viz graf 17. Pouze 39 dotazovaných osob (28,5 %) zásadně používá 3D Secure. 53 osoby uvedli, že ne používají služby (38,7 %). Ostatní respondenti nejsou u této otázky jistí (45 osob, 32,8 %). Záporné a nejisté odpovědi vyskytují napříč všemi socio-demografickými skupinami dotazovaných respondentů a nelze zde vymezit nějaký typ osob, který se ve svých odpovědích výrazně liší od ostatních.

Graf 17: Používáte službu 3D Secure?

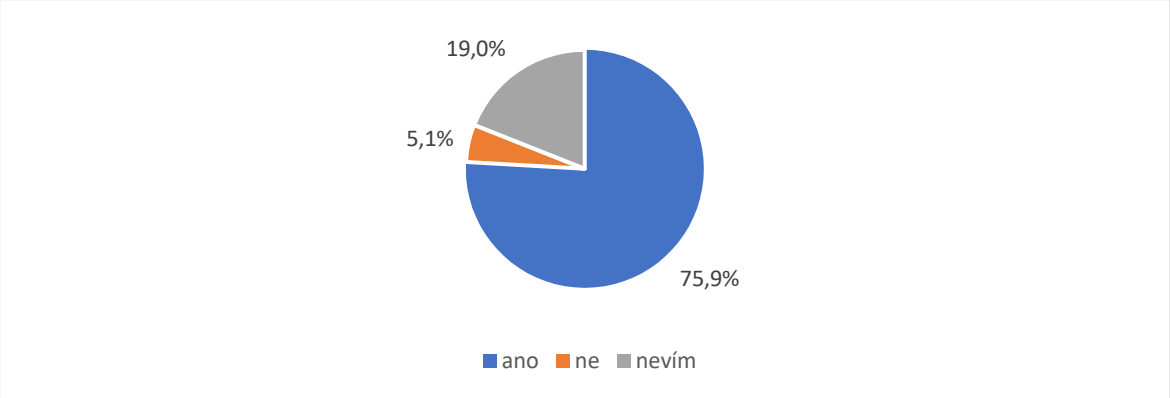


Zdroj: vlastní zpracování, 2023

Otázka č. 11: Umožňuje Vaše platební karta uplatnit tzv. chargeback (reklamace platby kartou online)?

Reklamace platbou kartou je užitečná v situacích, kdy byla karta zneužita podvodníkem nebo při placení u nespolehlivého obchodníka. Většina bank dnes tuto službu poskytuje. Povědomí o této službě je však nedostatečně vysoké mezi dotazovanými respondenty (viz graf 18). 26 osob (19 %) uvedli, že neví, zda jejich platební karta umožňuje uplatnit tzv. chargeback (reklamace platby kartou online) a 7 osob (5,1 %) se domnívá, že tuto možnost nemají.

Graf 18: Umožňuje Vaše platební karta uplatnit tzv. chargeback (reklamace platby kartou online)?



Zdroj: vlastní zpracování, 2023

Dále bylo prozkoumáno, jaké je povědomí o službě chargeback u dotazovaných klientů největších bank. Z výsledků průzkumu vyplývá, že nejvíce respondentů využívá platební karty od České spořitelny, ČSOB a AirBank. Odpovědi respondentů, kteří uvedli tyto banky, jsou uvedeny v tabulce 3. Je třeba zde upozornit na to, že někteří respondenti v průzkumu uvedli, že používají platební karty od více než 1 banky.

Je zřejmé, že mírně nižší povědomí o službě chargeback mají klienti České spořitelny (9 odpovědí „nevím“ a 2 odpovědí „ne“, tj. 25,6 % dotazovaných klientů této banky neví o této službě nebo se domnívá, že tuto službu nemají). Žádný z dotazovaných klientů ČSOB a pouze 1 klient AirBank se domnívá, že není jim tato služba poskytována. Dalších 6 klientů ČSOB (16,7 %) a 4 klienty AirBank (12,5 %) uvedli odpověď „nevím“.

Tabulka 3: Umožňuje Vaše platební karta uplatnit tzv. chargeback (reklamace platby kartou online) – rozdělení odpovědí klientů 3 nejpopulárnějších bank

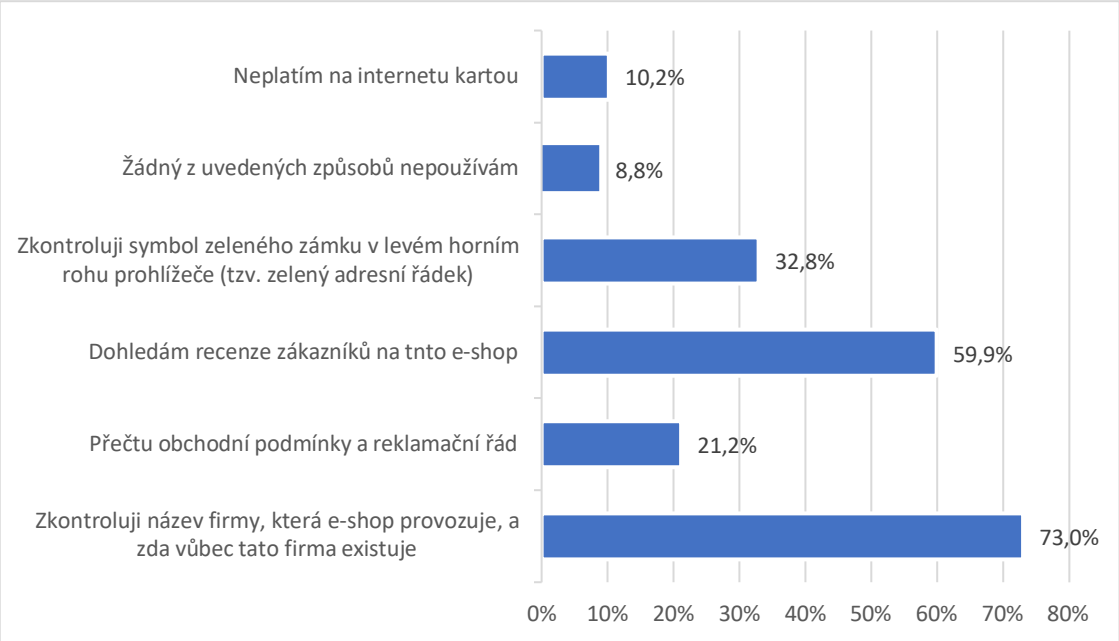
	Česká spořitelna	ČSOB	AirBank
Ano	32	30	27
Ne	2	0	1
Nevím	9	6	4
Celkem	**43**	**36**	**32**

Zdroj: vlastní zpracování, 2023

Otázka č. 12: Když platíte na internetu, ověřujete spolehlivost webových stránek prostřednictvím uvedených způsobů?

Několik jednoduchých zvyků při nakupování online může pomoci zvýšit bezpečnost platebních údajů. Vychází především z pozornosti vůči detailům a informacím na webových stránkách. V průzkumu byly uvedeny 5 možných způsobů kontroly spolehlivosti e-shopu – například kontrola zeleného zámku 3D secure, analýza zkušeností a recenzí jiných zákazníků, ověření firmy provozovatele webu atd. Respondenti mohli si zvolit jednu nebo více odpovědí, které nejlépe charakterizují jejich chování při nakupování online. Přehled odpovědí je znázorněn pomoci grafu 19.

Graf 19: Když platíte na internetu, ověřujete spolehlivost webových stránek prostřednictvím uvedených způsobu?



Zdroj: vlastní zpracování, 2023

Nejčastěji respondenti **kontrolují název firmy**, která provozuje e-shop (tuto odpověď si zvolilo 100 osob, 73 % výběrového souboru). Nelze zde však s jistotou tvrdit, že se jedná o pečlivou kontrolu názvu firmy (například vyhledávání ji na portálu Justice.cz nebo v seznamech nespolehlivých prodejců na internetu). Je možné, že kontrola firmy u části respondentů skončí na tom, že uvádí u její názvu označením s.r.o. nebo IČO. Není nikdy zaručeno, že jsou tyto údaje, uvedené na webu pravdivé, proto je lépe provést pečlivější kontrolu firmy.

Z porovnání odpovědí mužů a žen (viz tabulka níže) lze udělat závěr, že dotazováni muži častěji než ženy kontrolují název firem provozovatelů e-shopů (84,5 % mužů oproti 64,6 % žen). Vzhledem k tomu, že ve struktuře výběrového souboru jsou zastoupeny téměř ve stejné míře muži i ženy, lze tento závěr považovat za dost významný.

Dalším způsobem ověřit prodejce je dohledat **recenze jiných zákazníků**, tykající se jejich zkušeností s nakupováním. Je zde ovšem riziko, že na internetu jsou zveřejněny falešné recenze (nepravdivé, jsou napsány konkurenty nebo nejsou napsány skutečnými zákazníky atd.). Nicméně, pečlivé a subjektivní posouzení recenzí může zákazníkovi pomoci ověřit pravdivost informací. Horší je situace, kdy o prodejci nejsou žádné informace na internetu. V průměru 59,9 % dotazovaných respondentů (celkem 82 osob) uvedlo, že prohlíží recenze zákazníků před nákupem na internetu. Je také zřejmý rozdíl mezi zvyky mužů a žen: muži se zajímají o recenze zákazníků méně než ženy (30 mužů nebo 51,7 % oproti 52 ženám nebo 65,8 %).

Na třetím místě dle počtu odpovědí je kont**rola symbolu zeleného zámku v levém horním rohu prohlížeče** (45 osob, 32,8 %). Tento úkon je více typický pro chování mužů (22 mužů, 37,9 %) než žen (23 žen, 29,1 %).

Zhruba pětina respondentů (29 osob neboli 21,2 %) se věnuje pozornost **přečtení obchodních podmínek nebo reklamačního řádu** na webu e-shopu. Počet kladných odpovědí je zde relativně nižší než u jiných, výše pospaných úkonů, a rozdíly v chování mužů a žen jsou také nižší. Celkem 22,8 % žen a 19 % mužů uvedlo, že čte obchodní podmínky nebo reklamační řád na webu. Není zde však známo, jak pozorně jsou tyto dokumenty přečteny, a zda se jim věnována pozornost vždy nebo jenom při nákupu u nových prodejců.

10,2 % respondentů uvedlo, že neplatí na internetu kartou (i když z předchozích otázek vyplývá, že platební karty vlastní). Dalších 8,8 % respondentů uvedlo, že nepoužívají žádný z uvedených způsobů zvýšení bezpečnosti při platbách na internetu. Přehled odpovědí všech respondentů a také jejich rozdělení dle pohlaví respondentů je uvedeno v tabulce 4.

Tabulka 4: Když platíte na internetu, ověřujete spolehlivost webových stránek prostřednictvím uvedených způsobu? – rozdělení odpovědí dle pohlaví respondentů

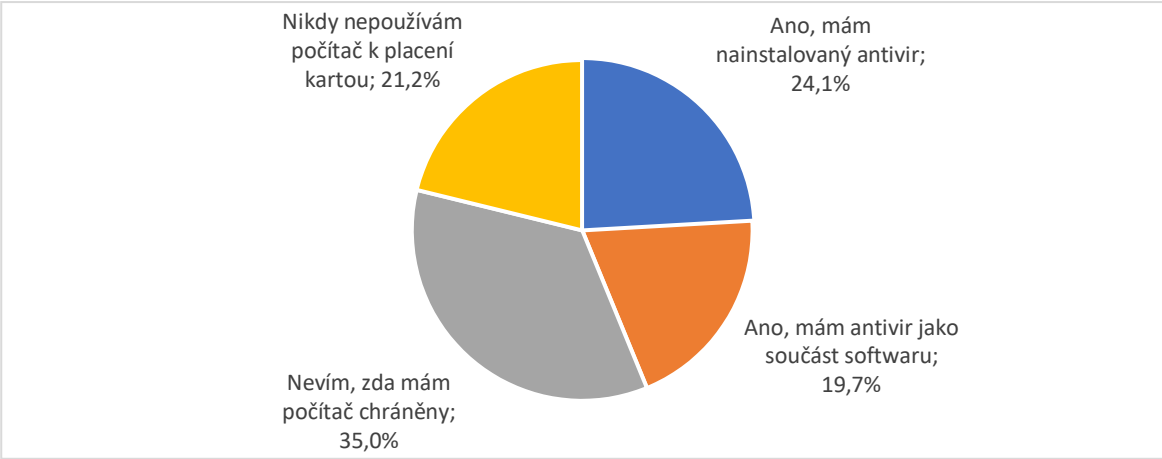
	Ženy (n=79)		**Muži (n=58)**		**Celkem (n=137)**	
Zkontroluji název firmy, která e-shop provozuje, a zda vůbec tato firma existuje	51	64,6 %	49	**84,5 %**	100	**73,0 %**
Přečtu obchodní podmínky a reklamační řád	18	22,8 %	11	19,0 %	29	21,2 %
Dohledám recenze zákazníků na tento e-shop	52	**65,8 %**	30	51,7 %	82	**59,9 %**
Zkontroluji symbol zeleného zámku v levém horním rohu prohlížeče (tzv. zelený adresní řádek)	23	29,1 %	22	**37,9 %**	45	32,8 %
Žádný z uvedených způsobů nepoužívám	5	6,3 %	7	12,1 %	12	8,8 %
Neplatím na internetu kartou	9	11,4 %	5	8,6 %	14	10,2 %

Zdroj: vlastní zpracování, 2023

Otázka č. 13: Pokud používáte **počítač** k placení kartou, máte toto zařízení chráněno proti napadení hackera?

Antivir je jednou z možností, jak chránit své zařízení proti útokům hackerů, různým vírům a krádeži informací. S rozvojem uživatelsky přátelských operačních systémů (zejména Mac OS) se stály běžní uživateli být méně zapojeni do „manuálního“ řízení svého počítače – stále méně pozornosti je od uživatelé vyžadováno pro to, aby instalovat nějaké speciální programy nad rámec standardního balíčku software v rámci operačního systému. Je proto pochopitelné, že 48 respondentů (35 %) neví, zda mají svůj počítač chráněný (viz graf 20). Dalších 33 osob (24,1 %) tvrdí, že mají nainstalovaný antivir, dalších 27 osob (19,7 %) považuje, že mají antivir jako součást software (platí to zejména pro MacBook, pracovní počítače). 29 osob (21,2 %) uvedlo, že nikdy nepoužívá počítač k placení kartou, což je odůvodněno trendem růstu využití přenosných zařízení pro online nakupování (tablety, mobily).

Graf 20: Pokud používáte počítač k placení kartou, máte toto zařízení chráněno proti napadení hackera?

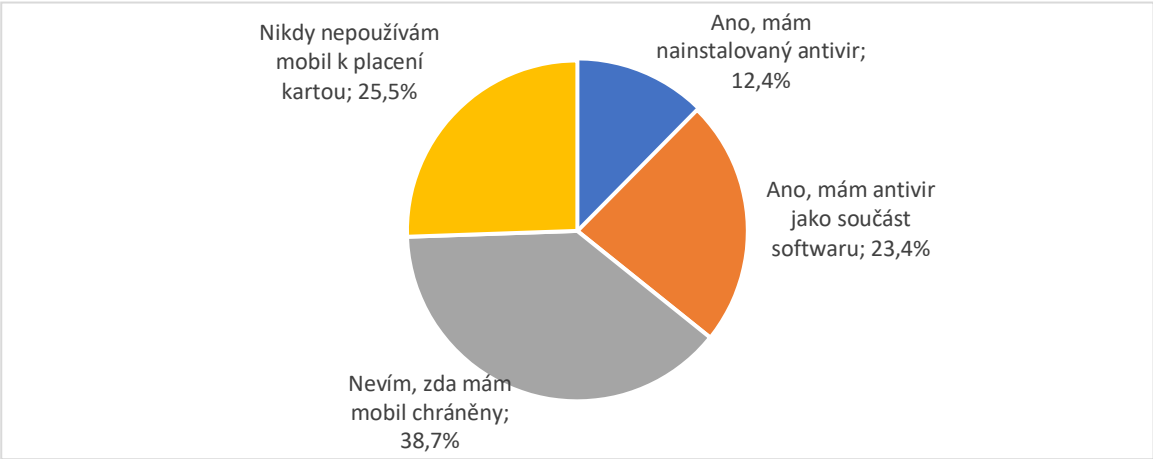


Zdroj: vlastní zpracování, 2023

Otázka č. 14: Pokud používáte **mobil** k placení kartou, máte toto zařízení chráněno proti napadení hackera?

Stejně jako počítač by měl mobil chráněn při využití placení kartou online. 53 respondentů (38,7 %) neví, zda má svůj mobil chráněny antivirem. 32 osoby (23,4 %) se domnívá, že mají antivir jako součást software, což je pravda pro většinu moderních mobilů. 17 osob (12,4 %) uvedlo, že mají navíc nainstalovaný antivir. 35 osob (25,5 %) uvedlo, že nepoužívá mobil při provedení plateb kartou. Toto číslo respondentů je překvapivě vyšší než u otázky využití počítače pro placení kartou. Přehled odpovědí respondentů je uveden pomoci grafu 21.

Graf 21: Pokud používáte mobil k placení kartou, máte toto zařízení chráněno proti napadení hackera?



Zdroj: vlastní zpracování, 2023

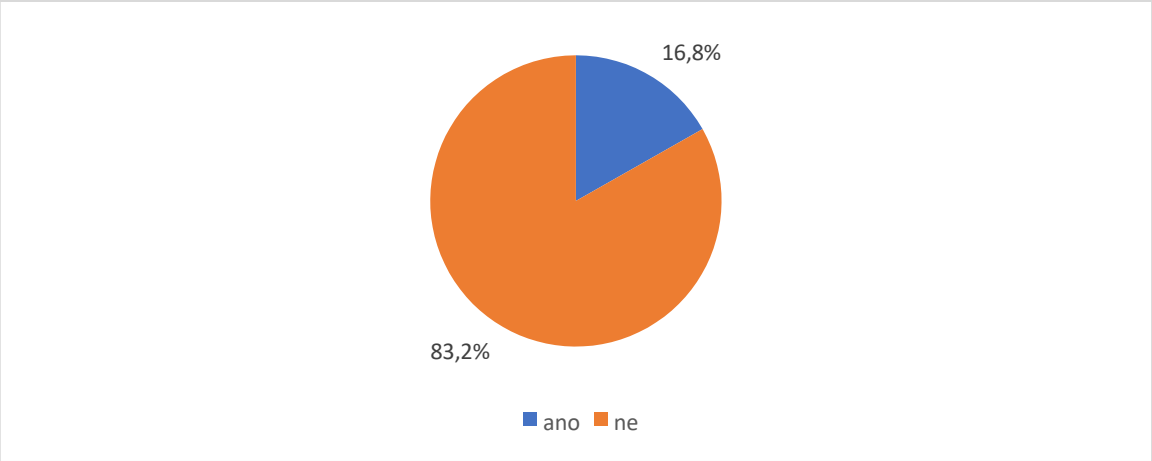
Povědomí respondentů o potřebě chránit svá zařízení antivirem, zejména pokud používají ho k placení kartou, je zatím hodnoceno jako nedostačující.

4.2.4 Povědomí o podvodech

Otázka č. 15: Setkal(a) jste někdy s podvodem s platebními kartami?

Další otázka byla polouzavřeného typu. Respondenti měli uvést, zda se někdy potkali s podvodem s platebními kartami, a pokud uvedli kladnou odpověď – krátce popsat tento případ, včetně následků tohoto podvodu (např. blokování karty, ztráta peněz apod.). Celkem 23 respondentů (16,8 %) uvedlo kladnou odpověď (viz graf 22) a následně krátce pospaly podvody, s nimiž se v minulosti setkali.

Graf 22: Setkal(a) jste někdy s podvodem s platebními kartami?



Zdroj: vlastní zpracování, 2023

Phishing – tento podvod byl přímo nebo nepřímo označen největším počtem respondentů (celkem 15 osob, z toho 6 žen a 9 mužů; 10,9 % výběrového souboru). Respondenti uvedli, že se jim volali podvodníci (z banků, policie apod.) a rozhovor vedl ve většině případů k prosbě poskytnout osobní údaje. V rámci rozhovoru nebyli respondenti přímo požádaní, aby poskytli údaje své karty, ale se domnívají, že podvod konečně je spojen s krádeží platebních údajů. Dále bylo zmíněno podvodní jednání „falešných“ obchodníků na Facebook (Market Place) a Bazos.cz. Bylo uvedeno, že komunikace někdy pokračovala v e-mailu a vedla k různým prosbám – zaplatit za zboží předem, uhradit poplatek spojený s dopravou apod.

Karta byla odcizená – platební karty byly odcizeny u 5 respondentů (3 ženy, 2 muži neboli 3,6 % všech respondentů). Důvody a následky odcizení byly různé, většina respondentů se však uvedla, že karta byla součástí odcizené kabelky, peněženky apod.

Bankomat zadržel platební kartu – tuto situaci uvedlo 3 respondenty (2 ženy a 1 muž, neboli 2,2 % všech respondentů). 1 respondentka navíc uvedla, že se zavolala na uvedenou kontaktní linku a situaci vyřešila. Ostatní respondenty nespecifikovali tuto situaci ani její následky.

V žádné z uvedených situací nebylo respondenty uvedeno, že kontaktovali policii.

Z výsledků lze udělat závěr, že se respondenti relativně vzácně potkávají s podvody s platebními kartami, což je dobře. Je však možné, že tento výsledek je způsoben neochotou respondentů sdílet informace, tj. ve skutečnosti se setkali s více podvodů, ale nechtějí je popisovat v průzkumu. Možná že si na tyto podvody v průběhu vyplňování dotazníku nevzpomenuli.

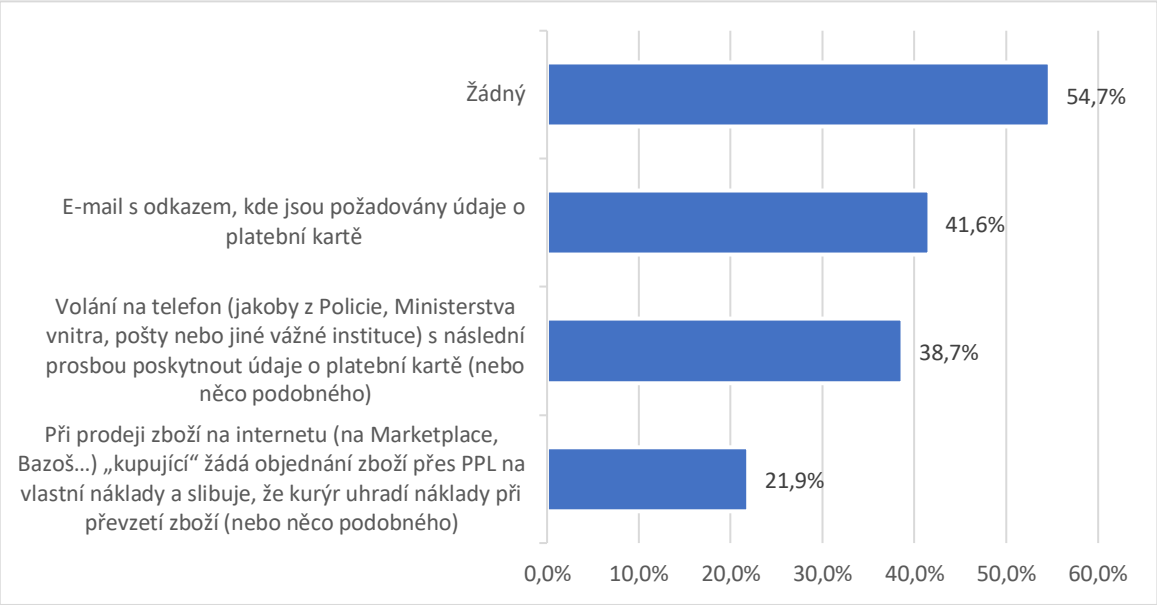
U předchozí otázky byli respondenti požádáni o to, aby popsali podvody, s nimiž se setkali. Vyžadovalo to spontánní znalost podvodů, tj. respondenti by měli být schopni samostatně odlišit podvodní případy od standardní situace v jejich životě. U následující otázky uzavřeného typu se jedná o zkoumání podpořené znalosti podvodů.

Otázka č. 16: Jaké z uvedených podvodů znáte / o nich jste někdy slyšel(a)? (lze si vybrat 1 nebo více odpovědí)

Bez ohledu na to, zda se osoba někdy v životě bezprostředně setkala s podvodníky, je důležitá všeobecné povědomí o rizikových situacích a podvodech. Pokud jedinec ví o možných podvodech s platebními kartami, může se lépe bránit výskytu těchto situací.

Stručně byly pospány tři relativně „populární“ podvody v ČR – při prodeji zboží na internetu, volání na telefon a podvodné e-maily. Respondenti jsou poměrně dobře obeznámeni s těmito podvody (viz graf 23 a tabulka 5).

Graf 23: Jaké z uvedených podvodů znáte / o nich jste někdy slyšel(a)?



Zdroj: vlastní zpracování, 2023

Tabulka 5: Jaké z uvedených podvodů znáte / o nich jste někdy slyšel(a)?

	Ženy (n=79)		**Muži (n=58)**		**Celkem (n=137)**	
Při prodeji zboží na internetu (na Marketplace, Bazoš…) „kupující“ žádá objednání zboží přes PPL na vlastní náklady a slibuje, že kurýr uhradí náklady při převzetí zboží (nebo něco podobného)	20	**25,3 %**	10	17,2 %	30	21,9 %
Volání na telefon (jakoby z Policie, Ministerstva vnitra, pošty nebo jiné vážné instituce) s následní prosbou poskytnout údaje o platební kartě (nebo něco podobného)	24	30,4 %	29	**50,0 %**	53	38,7 %
E-mail s odkazem, kde jsou požadovány údaje o platební kartě	27	34,2 %	30	**51,7 %**	57	41,6 %
Žádný	49	**62,0 %**	26	44,8 %	75	54,7 %

Zdroj: vlastní zpracování, 2023

Nejvíce respondentů uvedlo, že znají o **e-mailech** s odkazy a žádosti poskytnout platební údaje (57 osob, 41,6 %), přičemž mezi muži je toto povědomí vyšší než mezi ženy. Celkem 34,2 % žen a 51,7 % mužů uvedli kladnou odpověď.

Phishingová volání na telefon jsou také dost významně rozšířena v ČR. Zná o nich celkem 38,7 % dotazovaných respondentů (53 osob), z toho více mužů (29 osob nebo 50 % na celkovém počtu mužů) než žen (24 osoby nebo 30,4 % na celkovém počtu žen).

Přibližně pětina respondentů (30 osob, 21,9 %) zná **podvody při prodeji na platformách typů MarketPlace a Bazoš.** Mezi ženy je ználost těhco pdovodů vyšší než mezi muži (20 žen nebol 25,3 % na celkovém počtu žen oproti 10 mužům nebo 17,2 % na celkovém počtu mužů).

Mezi ženy obecně je však povědomí o podvodech nižší než mezi muži. Celkem 62 % žen a 44,8 % mužů uvedli, že neznají žádný z uvedených podvodů. Je třeba upozornit na to, že u výše uvedené otázky byla možnost si zvolit více než jednu variantu odpovědí. Vzhledem k tomu lze tvrdit, že mezi ženy jsou často respondentky, které znají více než jeden typ podvodu.

5. Zhodnocení výsledků a doporučení

Provedený průzkum se zaměřil na zhodnocení povědomí dotazovaných lidí z ČR o bezpečnosti využití platebních karet a možnostech ochrany proti podvodům. Z online průzkumu bylo využito 137 dotazníků, vyplněných respondenty, kteří splňují dvě základní podmínky (jedná se o záměrný výběr): a) respondent bydlí v ČR a b) využívá platební karty pro své nákupy. Vzorek není reprezentativní a nelze získané výsledky zobecnit na celou českou populaci. Poskytuje však zajímavé informace, vyplývající z názorů dost velkého počtu osob (137 respondentů). Ve struktuře respondentů je přibližně rovnocenné zastoupení mužů a žen, proto srovnání odpovědí respondentů dvou pohlaví je zejména cenné. Rozdělení respondentů do jiných soci-demografických skupin je méně rovnoměrné, proto nelze posoudit názory některých skupin respondentů (například seniorů, lidí se základním vzděláním, nezaměstnaných osob). Nejvíce jsou ve výběrovém vzorku zastoupeny následující osoby: studenty a zaměstnanci ve věku do 29 let se středoškolským nebo vysokoškolským vzděláním. Velký podíl respondentů tvoří především klienti dvou velkých bank v ČR – České spořitelny a ČSOB, a také modernější a menší banky AirBank. Lze také podotknout, že se respondenti vyznačují určitou počítačovou gramotností a jsou uživateli internetu, protože průzkum byl proveden formou online dotazníku.

Otázky v průzkumu byly rozděleny do tři základních skupin: způsoby využití platebních karet, bezpečnost platebních karet a povědomí o podvodech spojených s platebními kartami. Dále jsou uvedena klíčová zjištění z těchto oblastí průzkumu.

Respondenti využívají debetní platební karty v rámci svých nákupů velmi často (více než 90 % - denně nebo alespoň několikrát týdně). Mobilní telefony a chytré hodinky jsou pro účely placení používány menším počtem respondentů, ale v návaznosti na celosvětové trendy by mělo jejich využití růst. Respondenti také dost často používají počítače a mobily k placení na internetu a spíše menší část respondentů ví o tom, zda jsou jejich zařízení chráněna alespoň antivirem. Bezpečnost platebních karet a zařízení, používaných k placení, je pro respondenty velmi důležitá, vzhledem k aktivnímu využití těchto prvků v běžném životě.

Více než polovina respondentů by uvítala úplné omezení využití hotovosti v ČR a považuje bezhotovostní platební styk pohodlnější alternativou k hotovosti. Toto zjištění naznačuje růst významu bezpečnosti placení kartou pro respondenty.

Z průzkumu chování respondentů při využití bankomatů vyplývá, že rádi používají bezkontaktní přiložení karty (namísto vkládání karty do otvoru), což je bezpečnějším způsobem chování. Při vkládání peněz však respondenti preferují vkladomaty namísto návštěvy pobočky banky, což je méně bezpečný způsob chování.

Dále neuspokojivé výsledky byly zjištěny při analýze chování respondentů na internetu. Při nakupování v neznámém e-shopu je bezpečněji využívat platbu na dobírku nebo alespoň převod z účtu, který předpokládá možnost reklamace platby. Velká část respondentů však uvádí, že bude platit kartou online (17,5 %), nebo používat tlačítko bankovnictví (8 %) i u neznámých online prodejců, což je méně bezpečný způsob chování. Podíl mužů a žen na těchto odpovědích je zhruba stejný, proto nelze tvrdit, že by jedno pohlaví preferovalo méně bezpečnější platby.

Mezi bezpečnější platby jsou u žen populárnější platby na dobírku, u mužů – převod z účtu. Tyto výsledky nejsou příliš cenné z hlediska tvorby opatření pro bezpečnější využití plateb kartou, ale jsou velmi zajímavé z hlediska nákupního chování spotřebitelů.

Limit pro placení kartou je jedním z nejvíce rozšířených opatření v oblasti bezpečných plateb, která používají respondenty. Pozitivním výsledkem je také to, že si většina respondentů pamatuje svůj PIN kód a nemusí ho někdy psát do poznámek (což zvyšuje riziko krádeže).

Povědomí o možnostech využití pojištění platebních karet je hodnoceno jako nedostatečně vysoké, protože 39,4 % respondentů uvedlo u související otázky odpověď „nevím“. Z podrobné analýzy odpovědí bylo zjištěno, že odpovědi „ne“ a „nevím“ byly nejčastěji uvedeny respondenty s nižší úrovni vzdělání. Na základě toho je doporučeno, aby opatření, vedoucí ke zvýšení povědomí o možnostech pojištění platebních karet, byla zaměřena především na tyto rizikové skupiny respondentů. Doporučené je také upozornit na finanční výhodnost tohoto pojištění, protože faktor finančních nákladů může být pro tyto skupiny obyvatel velmi významný. Nízké povědomí o pojištění v tomto segmentu respondentů lze také spojit s jejich nižší finanční gramotností, avšak tato domněnka vyžaduje provedení dalšího průzkumu.

Nedostatečné je povědomí respondentů také v oblasti služby 3D Secure. Nebyly zjištěny zde rozdíly mezi socio-demografickými skupinami respondentů. V průměru méně než třetina dotazovaných osob ví, že používá tuto službu.

Služba chargeback – reklamace platby kartou online je dalším důležitým prvkem bezpečnosti, který poskytuje banka svému klientovi. Nicméně pouze tři čtvrtiny respondentů (75,9 %) ví o této službě. Některé rozdíly v názorech respondentů byly zjištěny při jejich rozdělení dle banky, jejíž klienty jsou. Například u klientů České spořitelny je povědomí o této službě nižší než u klientů ČSOB a AirBank. Nicméně počet dotazovaných klientů těchto bank je nízký (cca 30-40 osob u každé banky), proto kvalitu těchto výsledků může prokázat jen další rozsáhlejší výzkum.

Většina respondentů při nakupování online používá jako hlavní způsob ochrany proti podvodu kontrolu názvu firmy-provozovatele e-shopu (73 %). Není však zjištěno, jak kvalitní je tato kontrola, zda zahrnuje například vyhledávání firmy v obchodním rejstříku a seznamech nespolehlivých prodejců. Může to být další zajímavou oblastí výzkumu.

Pro více než polovinu respondentů (59,9 %) jsou důležité recenze ostatních zákazníků na internetu. Proto je obecným doporučením pro všechny uživatele e-shopů psát kvalitní a pravdivé recenze, které mohou pomoci identifikovat spolehlivé a nespolehlivé prodejce na internetu. Nahlášení podvodu policii a bance je také důležité z hlediska získání operativních informací a předcházení zneužití dat dalších lidí. Zatím z provedeného průzkumu vyplývá, že respondenti nedostatečně využívají možnosti šíření informací o podvodech.

V návaznosti na výsledky průzkumu je respondentům doporučeno zvýšit pozornost vůči symbolu 3D secure při nakupování online a také věnovat více pozornosti pečlivému přečtení obchodních podmínek jednotlivých online prodejců.

Při porovnání nakupování online u mužů a žen bylo zjištěno, že dotazované ženy častěji než muži používají recenze zákazníků jako zdroj informaci pro posouzení spolehlivosti prodejce. Dotazováni muži na rozdíl od žen častěji kontrolují názvy firem a symbol zeleného zámku v prohlížeči. Lze proto pro dotazované ženy doporučit věnovat více pozornosti také kontrole názvy firmy a symbolu zeleného zámku při nakupování online.

Z výsledků průzkumu vyplývá, že 16,8 % respondentů se někdy potkávalo s nějakými podvody ve spojení s placením kartou. Nejčastěji to byla phishingová volání, ale také i odcizení karty a zadržení karty bankomatem. Tento výsledek je třeba posuzovat s přihlédnutím ke spolehlivosti a pravdivosti odpovědí respondentů – je možné, že někdo nesdílel své zkušenosti. Podpořená znalost o existenci těchto podvodů (zejména phishingová volání a emaily) je u respondentů relativně vysoká, což lze hodnotit pozitivně. Nicméně povědomí o možných podvodech je vhodné neustále podporovat a aktualizovat.

Je třeba upozornit na to, že v rámci vlastního průzkumu a jiných studií jsou zkoumány jen některé oblasti bezpečnosti a chování proti podvodům s platebními kartami. Oblast kyberkriminality se však rychle vyvíjí, což souvisí s technologickým pokrokem, rozvojem umělé inteligence, analýzy dat apod. Současný výzkum a také vzdělání spotřebitelů v oblasti bezpečného využití platebních karet by měly dostat se napřed nebo alespoň držet krok s rozvojem kyberkriminality.

Je zřejmé, že nikdo není chráněn od všeho, co se stává ve světě. Ale zavedení alespoň několik jednoduchých zvyků do běžného života může pomoci zvýšit bezpečnost osobních dat a peněz každé osoby. Jedná se o pravidla, popsané například v kapitole 3.5 této práce – odmítnutí sdílení osobních dat 3. osobám, neopouštění prostoru bankomatu v případě zaseknutí karty, nastavení bezpečných limitů pro platby kartou, pojištění proti ztrátě a krádeže, pravidelná kontrola pohybu na účtu apod.

Vzhledem k růstu e-commerce je třeba věnovat zvýšenou pozornost spolehlivosti internetových prodejců. Několik málo času, věnovaného kontrole firmy provozovatele e-shopu nebo zákaznických recenzí může zachránit finance kupujícího.

Je třeba zmínit moderní hrozbu, spojenou s kyberútoky na databáze a stránky národních institucí, které uskutečňují hackeři ze zemí-účastnic válečných konfliktů. Útok může poškodit osobní data klientů bank, registrovaných uživatelů různých vládních portálů apod. Není proto doporučeno ukládat velké objemy citlivých dat, včetně údajů platebních karet na webových stránkách.

Za zmínku stojí také potřeba zvýšené pozornosti vůči možným podvodům při cestování do zahraničí. Zejména při návštěvě států mimo EU, méně rozvinutých zemí, neznámých společností s nezvyklou mentalitou je doporučeno byt zejména obezřetným při

využití bankomatů, nákupech online a placení kartou na POS-terminálech. Vyplatí se při cestování mít pojištění, které bude rozšířeno na situace, spojené se ztrátou platební karty, peněz apod.

6. Závěr

Bakalářská práce byla věnována aktuálnímu tématu bezpečnosti platebních karet. Lidé se potkávají s podvody při placení kartou online, na POS-terminálech, při využití bankomatů a vkladomatů. Technologický pokrok a rostoucí kyberkriminalita zvyšuje význam ochrany proti podvodům v oblasti bezhotovostních plateb. Vzhledem k trendu rozšíření využití placení kartou, který vyplývá z analýzy statistik platebního styku v ČR, je bezpečnost platebních karet důležitou problematikou pro každého obyvatele země.

Hlavním cílem práce bylo vymezit způsoby ochrany platebních karet (PK) v České republice, nastínit historii jejich vývoje v celém světě a přímo v ČR a zjistit současný stav ochrany PK ze strany držitele a ze strany banky, která karty vydala. Tento cíl byl naplněn především v rámci literární rešerše v první části práce, která obsahuje přehled historii PK, charakteristiku legislativy a opatření ve vztahu k ochraně PK, popis konkrétních způsobů ochrany proti podvodům.

Vedlejším cílem práce bylo zhodnocení povědomí dotazovaných lidí v ČR o podvodech, spojených s využitím PK, a možnostech ochrany proti nim. V návaznosti na výsledky literární rešerše byl vytvořen online dotazník, který umožnil prozkoumat zkušenosti a názory 137 mladých lidí z ČR vůči tomu, jaké prvky bezpečnosti při placení kartou využívají ve svém běžném životě. V práci byly porovnány názory dotazovaných mužů a žen, klientů různých bank, hledány rozdíly v názorech respondentů s různou úrovní vzdělání a typem činností. Díky tomu bylo možné nalézt odpověď na výzkumnou otázku (Jaké skupiny respondentů jsou nejlépe informování o možnostech ochrany proti podvodům, spojeným s PK?).

Bylo zjištěno, že nejnižší povědomí o pojištění platebních karet, které je jedním z prvků ochrany proti podvodům, mají dotazovaní lidé s nižší úrovní vzdělání. Informační úsilí bank, zaměřená na růst povědomí o pojištění platebních karet, je proto vhodné zacílit na tento segment dotazovaných osob. Je doporučeno zdůraznit finanční výhodnost nabídky pojištění, protože faktor ceny může být pro tyto osoby důležitým. Z výsledků průzkumu vyplývá – ženy méně než muži využívají některé prvky kontroly spolehlivosti online prodejce a proto v návaznosti na zjištěné výsledky byla vytvořena některá doporučení pro jejich chování (například věnovat více pozornosti kontrole firmy-provozovatelů e-shopů, obchodním podmínkám a symbolu 3D secure na webu).

7. Seznam použitých zdrojů

BARTONŇ STUDIO. 2021, 29. dubna. Silné ověřování online plateb. Jak se to dotkne e-shopů a zákazníků? *Bartoň Studio.* [online]. [cit. 2022-10-20]. Dostupné z WWW: <https://www.bartonstudio.cz/silne-overovani-online-plateb/>

BELÁS, J., DEMJAN, V. 2014. Bank customers satisfaction: Case studies from Czech Republic. *Actual problems of economics*, 12(162): 315–323. ISSN 1993-6788.

BHATLA T., PRABHU, V., DUA, A. 2003. *Understanding credit card frauds.* Tata Consultancy Services. Dostupné z: https://popcenter.asu.edu/sites/default/files/problems/credit_card_fraud/PDFs/Bhatla.pdf

ČBA, 2021, 24. červen. *Průzkum ČBA: Češi a platební styk 2021.* [online]. [cit. 2022-10-20]. Dostupné z WWW: <https://cbaonline.cz/pruzkum-cba-cesi-a-platebni-styk-2021>

ČESKO. Zákon č. 370/2017 Sb., o platebním styku – znění od 1. 7. 2022. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2023 [cit. 2023-1-2]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2017-370>

ČNB. 2021, 4. ledna. Silné ověření uživatele u plateb kartou na internetu od 1.1.2021. In: *Česká národní banka.* [online]. [cit. 2023-1-2]. Dostupné z: <https://www.cnb.cz/cs/dohled-financni-trh/vykon-dohledu/upozorneni-pro-verejnost/Silne-overeni-uzivatele-u-plateb-kartou-na-internetu-od-1.-1.-2021/>

ČNB, 2023. Statistika platebních styku. *Databáze ARAD*. [online]. [cit. 2023-2-10]. Dostupné z: <https://www.cnb.cz/cnb/STAT.ARADY_PKG.STROM_SESTAVY?p_strid=AAAE&p_sestuid=&p_lang=CS>

ČSOB. 2022. Pojištění internetových rizik. *ČSOB.* [online]. [cit. 2022-12-30]. Dostupné z WWW: <https://www.csob.cz/portal/lide/pojisteni/pojisteni-internetovych-rizik>

ČSOB. 2023. Jak bezpečně využívat platební karty? In: *ČSOB.cz.* [online]. [cit. 2022-10-20]. Dostupné z WWW: <https://www.csob.cz/portal/bezpecnost/zasady-bezpecneho-chovani/jak-bezpecne-vyuzivat-platebni-karty>

ČT24. 2014, 21. října. Platební karta slaví stovku a míří k bezkontaktnosti. *ČT24*. [online]. [cit. 2022-11-11]. Dostupné z WWW: <https://ct24.ceskatelevize.cz/ekonomika/1012810-platebni-karta-slavi-stovku-a-miri-k-bezkontaktnosti>

DVOŘÁK, P. 2005. *Bankovnictví pro bankéře a klienty*. Praha: Linde. 688 s. ISBN 80-720-1515-X.

EDITORCZ MASTERCARD. 2021, 19. srpna. Mastercard končí s magnetickými proužky na platebních kartách. *Masercard.cz*. [online]. [cit. 2022-11-13]. Dostupné z WWW: <https://www.mastercard.com/news/europe/cs-cz/tiskove-centrum/tiskove-zpravy/cs-cz/2021/srpen/mastercard-konci-s-magnetickymi-prouzky-na-platebnich-kartach/>

ESET. 2022. Co je Phishing? In: *Eset.com*. [online]. © 1992 – 2023 ESET. [cit. 2022-10-20]. Dostupné z WWW: <https://www.eset.com/cz/phishing/>

EVROPSKÁ KOMISE. 2017. Nařízení komise v přednesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017. In: *Úřední věstník Evropské unie L 69/23*. [online]. [cit. 2023-1-3]. Dostupné z WWW: <https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1520948030732&uri=CELEX:32018R0389>

GARDLÍKOVÁ, M. 2019, 10. října. Silné ověření uživatele. In: *ePravo.cz*. [online]. © EPRAVO.CZ – Sbírka zákonů, judikatura, právo. [cit. 2023-1-3]. Dostupné z WWW: <https://www.epravo.cz/top/clanky/silne-overeni-uzivatele-110056.html#_ftn2>

GOLD, S. 2014. The Evolution of Payment Card Frud. *Computer Fraud & Security*, March 2014(3): 12-17. https://doi.org/10.1016/S1361-3723(14)70471-3.

HOVORKOVÁ, K. 2018. Vypadají jako nástroj moderní doby. Přitom platební karty pamatují už víc než sto let. *Aktuálně.cz*. [online]. [cit. 2022-11-11]. Dostupné z WWW: <https://zpravy.aktualne.cz/ekonomika/platebni-karty-pamatuji-uz-vic-nez-sto-padesat-let/r~01ca4fbaee3d11e8a1900cc47ab5f122/v~sl:4c1b81909e39fc6feea6b3e69e60fbed/>

HRDINA, R. 2022, 21. března. Podvody na internetových bazarech. In: *Policie České republiky*. [online]. [cit. 2022-10-20]. Dostupné z WWW: <https://www.policie.cz/clanek/podvody-na-internetovych-bazarech.aspx>

JCB. 2021. History. *Global Website JCB*. [online]. [cit. 2022-11-11]. Dostupné z WWW: <https://www.global.jcb/en/about-us/history/>

JÍLEK, J. 2013. *Finance v globální ekonomice I: Peníze a platební styk*. Praha: Grada Publishing. 664 s. ISBN 978-80-247-8821-0.

JUŘÍK, P. 2005. Kdo vydal první univerzální platební kartu. *iDnes.cz*. [online]. [cit. 2022-11-13]. Dostupné z WWW: <https://www.idnes.cz/finance/banky-a-sporeni/kdo-vydal-prvni-univerzalni-platebni-kartu.A051005_160244_fi_osobni_zal>

JUŘÍK, P. 2012. *Platební karty: ilustrovaná historie placení*. Praha: Libri. 204 s. ISBN 978-80-727-7498-2.

KALABIS, Z. 2015, 4. listopadu. Střípky z historie platebních karet a bankomatů. *Zlatá koruna*. [online]. [cit. 2022-11-11]. Dostupné z WWW: <http://www.zlatakoruna.info/zpravy/ucty/stripky-z-historie-platebnich-karet-bankomatu>

KAPITOL. 2016, 9. června. Nelegální kopírování platebních karet – skiming. In: *Kapitol.cz.* [online]. [cit. 2022-10-20]. Dostupné z WWW: <https://www.kapitol.cz/magazin/nelegalni-kopirovani-platebnich-karet-skimming/>

KARGINA, L. Prospects for the development of electronic payment systems. *Transport Business in Russia,* 11: 12-13. ISSN 2072-8689.

KOLOUCH, J. 2003. *Cyber Crime*. Mason Crest Publishers. ISBN 978-80-881-6816-4.

KORAUŠ, A. a kol. 2017. The dafety risks related to bank cardsd and cyber attacks. Journal of Security and Sistainability Issues, 6(4): 563-574. http://doi.org/10.9770/jssi.2017.6.4(3).

KRIVINŠ, A. 2015. Towards security and safety: police efficiency across European countries. *Journal of Security and Sustainability Issues*, 5(1): 35-44. http://doi.org/10.9770/jssi.2015.5.1(3).

KUZNETSOV, D. 2007. Istorija vozniknovenija, klassifikacija i pravovaje voprosy ispol'zovanija i zashity bankovskich platežnych kart. *Vestnik Sankt-Peterburgskogo universiteta MVD Rossii*. 2(34): 27-35. ISSN 2071-8284.

LOHNERT, M. 2021, 22. listopadu. Hackeři vědí, jak obejít dvoufázové ověření. Útok je jednoduchý, jak se bránit? *inSmart*. https://insmart.cz/bezpecnost-dvoufazoveho-overeni-phishing/

MARTIŠKOVÁ, V. 2018, 26. listopadu. Platební karty. *DU.cz*. [online]. [cit. 2022-10-20]. Dostupné z WWW: <https://www.du.cz/33/platebni-karty-uniqueidmRRWSbk196FNf8-jVUh4Emsy4iYjEZCSEf_hPvJaVzA/>

MICROSOFT. 2022. Druhy podvodů s platebními kartami. In: *Microsoft: Dynamics 365*. [online]. [cit. 2022-10-20]. Dostupné z WWW: <https://dynamics.microsoft.com/cs-cz/ai/fraud-protection/credit-card-fraud/>

MONETA. 2023. Co je předplacená karta? *Moneta Money Bank*. [online]. [cit. 2022-11-11]. Dostupné z WWW: <https://www.moneta.cz/slovnik-pojmu/detail/co-je-predplacena-karta>

PEKER, S.; TVARONAVIČIENĖ, M.; AKTAN, B. 2014. Sustainable risk management: fuzzy approach to volatility and application on FTSE 100 index. *Entrepreneurship and Sustainability Issues*, 2(1): 30-36. http://dx.doi.org/10.9770/jesi.2014.2.1(4).

PLISCHKE, E. 2007, 27. dubna. Jak došly platební karty do českých zemí aneb historie karet plná zajímavostí. *Peníze.cz*. [online]. [cit. 2022-11-11]. Dostupné z WWW: <https://www.penize.cz/platebni-karty/18777-jak-dosly-platebni-karty-do-ceskych-zemi-aneb-historie-karet-plna-zajimavosti>

POLICIE ČR. 2022. Co je skimmovací zařízení? In: *Policie České republiky.* [online]. [cit. 2022-10-20]. Dostupné z WWW: <https://www.policie.cz/clanek/co-je-skimmovaci-zarizeni.aspx>

POLICIE.CZ. 2021, červen. Vishing a spoofing. In: *Policie České republiky*. [online]. [cit. 2022-10-20]. Dostupné z WWW: <https://www.policie.cz/clanek/vishing-a-spoofing.aspx>

POLOUČEK, S. 2006. *Bankovnictví*. Praha: C. H. Beck. 716 s. ISBN 80-7179-462-7.

SBK. 2012. Pofil České republiky. *Sdružení pro bankovní karty*. [online]. [cit. 2022-10-20]. Dostupné z WWW: <http://www.bankovnikarty.cz/pages/czech/profil_cr.html>

Systém proti skimmingu. In: *CZ Protect.* [online]. [cit. 2023-1-4]. Dostupné z WWW: <http://www.czprotect.cz/cs/content/17-system-proti-skimmingu>

ŠTITILIS, D., KLIŠAUSKAS, V. 2015. Aspets of cybersecurity: the case of legal regulation in Lithuania. *Journal of Security and Sustainability Issues,* 5(1): 45–57. http://dx.doi.org/10.9770/jssi.2015.5.1(4).

ŠVARCOVÁ, J. 2019. Platební karty. In: *Bankovnictví*. [online]. [cit. 2022-10-20]. Dostupné z WWW: <http://www.ceed.cz/bankovnictvi/769platebni_karty.htm>

ZENDULKA, J. 2022, 3. února. Nová vlna podvodů s platebními kartami. Vykukové „jdou“ po inzerentech nabízejících k prodeji použité věci. In: Kurzy.cz. [online]. [cit. 2022-10-20]. Dostupné z WWW: <https://www.kurzy.cz/zpravy/632551-nova-vlna-podvodu-s-platebnimi-kartami-vykukove-jdou-po-inzerentech-nabizejicich-k-prodeji/>

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

8.2 Seznam tabulek

8.3 Seznam grafů

Přílohy

Odkazovaný seznam příloh

Příloha A: Dotazník

Dotazník je zpracováván v rámci bakalářské práce na České zemědělské univerzitě v Praze. Jeho tématem je bezpečnost platebních karet v ČR. Dotazník je určen pouze osobám, které používají platební karty pro své nákupy. Není třeba vyplňovat dotazník, pokud platební kartu nevyužíváte. Dotazník je anonymní a nevyžaduje žádné osobní informace, jejíchž poskytnutí by mohlo nějakým způsobem Vás poškodit.

Předem děkuji za věnovaný čas.

1. Platební kartu jaké banky využíváte v současné době? (pokud používáte více platebních karet, uveďte max. 3 banky, které využíváte nejvíce)
   a) Česká spořitelna
   b) KB
   c) ČSOB
   d) AirBank
   e) Raiffeisenbank
   f) Moneta
   g) Fio
   h) Equa
   i) mBank
   j) …….

2. Jak často využíváte uvedené způsoby placení?

	Nikdy	1x za půlroku nebo vzácněji	Cca 1x	Cca 1x týdně	Několikrát týdně	Denně	Nevím
Hotovost							
Debetní platební karta							
Kreditní karta							
Mobilní telefon (Apple Pay, Google Pay…)							
Chytré hodinky							
Platební „známka“ na mobilu, klíčích…							

3. Co si myslíte o tom, kdyby přestala existovat hotovost? Pro odpovědi použijte následující škálu, kde:

1 znamená „Rozhodně bych to neuvítal(a); je to omezení svobody“,

5 znamená „Půl na půl“,

10 znamená „Uvítal(a) bych to; je to zjednodušení života“.

4. Při výběru hotovosti z bankomatu, jaký z uvedených způsobů používáte (za předpokladu, že máte k dispozici obě možnosti)?
   a) Vložím kartu přímo do bankomatu
   b) Bezkontaktní (přeložení karty nebo mobilu k čtečce v bankomatu)

5. Pokud potřebujete vložit hotovost na účet a máte k dispozici obě dále uvedené možnosti, jaký způsob preferujete:
   a) Použiji vkladomat
   b) Raději zajdu na pobočku banky

Bezpečnost platebních karet

6. Pokud u neznámého internetového prodejce nakupujete poprvé, jaký způsob placení s největší pravděpodobností zvolíte?

a) Na dobírku
b) Převod z účtu
c) Platební kartou online
d) Přímá platba z bankovnictví na stránkách prodejce
e) E-peněženka (např. PayPal)
f) Nevím

7. Máte nastavený limit pro platby kartou?
    a) Ano
    b) Ne
    c) Nevím

8. Máte platební kartu pojištěnou proti ztrátě a odcizení?
    a) Ano
    b) Ne
    c) Nevím

9. Pamatujete si svůj PIN kód k platební kartě?
    a) Ano
    b) Ne

10. Používáte službu 3D Secure?
    a) Ano
    b) Ne
    c) Nevím

11. Umožňuje Vaše platební karta uplatnit tzv. chargeback (reklamace platby kartou online)?
    a) Ano
    b) Ne
    c) Nevím

12. Když platíte na internetu, ověřujete spolehlivost webových stránek prostřednictvím uvedených způsobu?
    a) Zkontroluji název firmy, která e-shop provozuje, a zda vůbec tato firma existuje
    b) Přečtu obchodní podmínky a reklamační řád
    c) Dohledám recenze zákazníků na tento e-shop
    d) Zkontroluji symbol zeleného zámku v levém horním rohu prohlížeče (tzv. zelený adresní řádek)

e) Žádný z uvedených způsobů nepoužívám
f) Neplatím na internetu kartou

13. Pokud používáte **počítač** k placení kartou, máte toto zařízení chráněno proti napadení hackera?
    a) Ano, mám nainstalovaný antivir
    b) Ano, mám antivir jako součást softwaru
    c) Nevím, zda mám počítač chráněny
    d) Nikdy nepoužívám počítač k placení kartou

14. Pokud používáte **mobil** k placení kartou, máte toto zařízení chráněno proti napadení hackera?
    e) Ano, mám nainstalovaný antivir
    f) Ano, mám antivir jako součást softwaru
    g) Nevím, zda mám mobil chráněny
    h) Nikdy nepoužívám mobil k placení kartou

Povědomí o podvodech

15. Setkal(a) jste někdy s podvodem s platebními kartami?
    a) Ano
    b) Ne

    Pokud jste se setkal(s) někdy s podvodem s PK, prosím, krátce popište tento případ:

    ……

    A uveďte, s jakými následky podvodu jste se setkal (např. blokování karty, ztráta peněz, kontaktování policie atd.).

    ……

16. Jaké z uvedených podvodů znáte / o nich jste někdy slyšel(a)? (lze si vybrat 1 nebo více odpovědí)
    a) Při prodeji zboží na internetu (na Marketplace, Bazoš…) „kupující“ žádá objednání zboží přes PPL na vlastní náklady a slibuje, že kurýr uhradí náklady při převzetí zboží (nebo něco podobného)
    b) Volání na telefon (jakoby z Policie, Ministerstva vnitra, pošty nebo jiné vážné instituce) s následní prosbou poskytnout údaje o platební kartě (nebo něco podobného)
    c) E-mail s odkazem, kde jsou požadovány údaje o platební kartě
    d) Žádný

Základní charakteristika respondentů

17. Vaše pohlaví:
    a) Žena
    b) Muž

18. Váš věk:
    a) …-19 let
    b) 20-29 let
    c) 30-39 let
    d) 40-49 let
    e) 50-59 let
    f) 60-69 let
    g) 70-… let

19. Vaše nejvyšší dosažené vzdělání:
    a) Bez vzdělání / neúplné základní
    b) Základní
    c) Střední bez maturity
    d) Střední s maturitou
    e) Vyšší odborné

f) Vysokoškolské

20. Hlavní činnosti v současné době:
    a) Student
    b) Zaměstnanec
    c) Podnikatel
    d) Na mateřské / rodičovské / otcovské dovolené
    e) Důchod
    f) Nezaměstnaný

Zdroj: vlastní zpracování, 2023