VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

ÚSTAV SOUDNÍHO INŽENÝRSTVÍ

INSTITUTE OF FORENSIC ENGINEERING

SYSTÉMOVÉ POJETÍ RIZIK SPOJENÝCH S VEDENÍM BANKOVNÍHO ÚČTU

SYSTEM APPROACH TO RISKS ASSOCIATED WITH BANK ACCOUNT MANAGEMENT

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. Denisa Hájková

AUTHOR

VEDOUCÍ PRÁCE — prof. Ing. Přemysl Janíček, DrSc.

SUPERVISOR

BRNO 2017

Vysoké učení technické v Brně, Ústav soudního inženýrství

Akademický rok: 2016/17

ZADÁNÍ DIPLOMOVÉ PRÁCE

student(ka): Bc. Denisa Hájková

který/která studuje v **magisterském studijním programu**

obor: **Řízení rizik firem a institucí (3901T048)**

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma diplomové práce:

Systémové pojetí rizik spojených s vedením bankovního účtu

v anglickém jazyce:

System Approach to Risks Associated with Bank Account Management

Stručná charakteristika problematiky úkolu:

Úkol, který se bude řešit je problémem, protože není obecně známo, jak se tento úkol řeší. Popis problému je obsažen v zadání.

Cíle diplomové práce:

V současnosti sice existuje soupis rizik, která souvisejí s vedením bankovního účtu, k těmto rizikům se však nepřistupuje systémově, protože se obecně neví (v praxi i na VŠ), co to vlastně znamená. Tuto situaci je nutno změnit, což bude realizováno v diplomové práci. Cílem diplomové práce je vypracovat systémové pojetí rizik spojených s vedením bankovního účtu, aby se odstranila neznalost existující v této oblasti a tedy vyřešila se příslušná problémová situace. Pokud se toto podaří splnit, bude mít diplomová práce charakter práce disertační, protože přinese nové poznatky.

Seznam odborné literatury:

Doporučuji literaturu, která souvisí s problematikou systémové metodologie, s níž je diplomantka seznámena. Odbornou literaturu oblasti bankovnictví si vyhledá diplomantka. Vysokoškolák musí být totiž natolik erudovaný, že si potřebnou literaturu vyhledá v rámci rešeršních analýz, čímž současně zjistí, na jaké úrovni poznání je v současnosti řešená problematika a využije to k řešení.

Vedoucí diplomové práce: prof. Ing. Přemysl Janíček, DrSc.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2016/17.

V Brně, dne 21. 10. 2016

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
ÚSTAV SOUDNÍHO INŽENÝRSTVÍ

doc. Ing. Aleš Vémola, Ph.D.
ředitel vysokoškolského ústavu

Abstrakt

Základem diplomové práce je změnit nestandardní problémovou situaci na standardní s využitím zvýšení finanční gramotnosti klientů bank ve vztahu k vedení účtu. Literární rešerše je zaměřená na bankovní a technologické pojmy, dále je doplněna o znalosti týkající se rizika. Za hlavní přínos práce považuji vytvoření souboru jednotlivých rizik a jejich kategorizaci, která byla vytvořena na základě získané praxe. Dále bylo v diplomové práci provedeno dotazníkové šetření a následně statisticky zpracováno.

Abstract

The basis of this thesis is to change the non-standard problem situation into a standard situation by using an increase of financial literacy of the bank's clients in relation to the account management. The literary research focuses on banking and technological concepts, supplemented by increased risk knowledge. The main contribution of my work is the creation of a set of individual risks and their categorization, which was created based on my gained practical experience. In addition, this thesis comprises of a survey which was carried out in the thesis and then statistically analyzed.

Klíčová slova
Problémová situace, problém, banky, rizika spojená s vedením bankovního účtu, rizika přímo ovlivnitelná klientem, rizika nepřímo ovlivnitelná klientem, rizika umělá rizika, chování klientů bank ve vztahu k bankovnímu účtu

Keywords

Problem situation, problem, banks, risks associated with bank account management, risks directly influenced by the client, risks indirectly influenced by the client, risks, artificial risk, behavior of bank clients in relation to the bank account

Bibliografická citace VŠKP

HÁJKOVÁ, D. *Systémové pojetí rizik spojených s vedením bankovního účtu*. Brno: Vysoké učení technické v Brně, Ústav soudního inženýrství, 2017. 66 s. Vedoucí diplomové práce prof. Ing. Přemysl Janíček, DrSc..

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval(a) samostatně a že jsem uvedl(a) všechny použité informační zdroje.

V Brně dne 25. 5. 2017

.....

podpis autora
Bc. Denisa Hájková

Poděkování

Ráda bych touto cestou poděkovala svému vedoucímu, který při mne vždy stál a poskytoval mi nesmírnou podporu při tvorbě této diplomové práce. Dále bych chtěla poděkovat všem lidem, kteří byli mojí oporou a pomáhali mi při studiu i v životě.

Obsah

1 Úvod a cíl práce

1.1 Úvod

S riziky se v běžném životě setkáváme prakticky každý den. Rizika jsou součástí našich životů, i když si to mnohdy zcela neuvědomujeme. Nicméně neuvědomování si rizika může mít v určitých oblastech zcela fatální následky.

Jedním z typických příkladů je vytváření rizik nevědomky, avšak svým chováním, vedoucím například ke zneužití vlastního bankovního účtu. I přes všechna bezpečnostní opatření, která nám poskytují bankovní instituce se může stát, že i běžný občan tato rizika vlastním chováním opět zvýší.

Mezi nejčastější rizikové chování můžeme řadit špatné úsudky majitelů účtů, ať už se jedná o účty vedené v České republice nebo kdekoli ve světě. Protože je tento problém rozsáhlý, je nezbytné mu věnovat patřičnou pozornost a snažit se tato rizika snížit nebo zcela odstranit.

1.2 Cíl práce

Cílem této diplomové práce je identifikovat rizika spojená s vedením bankovního účtu, která jsou přímo ovlivnitelná klientem a navrhnout patřičná opatření pro jejich snížení nebo je zcela odstranit.

2 Problémová situace

V České republice, ale i kdekoli ve světě, lidé využívají bankovních účtů pro hospodaření se svými financemi. Přestože existuje nespočet institucí, které nabízejí možnost uložení financí, ne každý je nakloněn k jejich využití.

Otázkou zůstává, zda je pro jedince přijatelnější nést riziko spojené s držením hotovosti anebo rizika, která se vztahují k uložení financí na bankovní účet? Každá z těchto možností přináší různá úskalí, která by mohla jedince při rozhodování ovlivnit. Avšak v případě uložení financí do banky je velká část rizik přenesena na tuto instituci.

Protože ne každý jedinec je interesován do vysoké míry zodpovědnosti, předpokládejme, že bude výhodnější finance vložit na bankovní účet, a tím přenést co nejvíce rizik na vybranou bankovní instituci. Ostatně tato hypotéza byla potvrzena studií od České bankovní asociace, která proběhla v roce 2016. Dle České bankovní asociace (2016) roste oblíbenost platby kartou oproti platbě hotovostí. Za posledních 10 let se poměr bezhotovostních transakcí zvýšil, je téměř čtyřnásobný. Dlouhodobě klesá i počet výběrů z bankomatu, jejich se počet za posledních 10 let snížil o 63 %. Pokles byl zaznamenán i u takzvaných cash back, tedy výběru hotovosti přímo na pokladně obchodníka. Meziročně se jednalo o 76% propad v objemu. [2]

I když velká část obyvatelstva účet používá, neznamená to však, že je v České republice vysoká míra finanční gramotnosti. Na webových stránkách Ministerstva financí České republiky (2016) je uvedeno, že provedli ke konci roku 2015 měření úrovně finanční gramotnosti dospělé populace České republiky. Toto šetření se stalo součástí světového měření společně s dalšími desítkami zemí Organizace pro hospodářskou spolupráci a rozvoj (OECD). Výsledkem tohoto šetření bylo, že finanční neznalost u nás převažuje nad finanční znalostí. [1] Toto zjištění může mít za následek nevědomé zvyšování rizik při manipulaci s účtem ze strany klientů.

Lidé využívají pro ukládání svých financí bankovní účty, které jsou zabezpečeny samotnými institucemi. Existují však rizika, která banky ovlivnit nedokáží. Jedná se zejména o ta, která si způsobují samotní klienti – uživatelé služeb, které banka nabízí. Pro běžného občana to znamená, že při využívání bankovního účtu může nevědomky vytvářet situace, které by následně vedly ke zneužití jeho bankovního účtu.

Nestandardnost situace je tedy v nízké finanční gramotnosti klientů bank. Zvýšením vědomosti klientů lze tato rizika alespoň částečně snížit, konkrétně navýšením jejich finanční gramotnosti ve vztahu k vedení účtu, a tím udělat situaci standardní.

2.1 Problém

Je nezbytné zvýšit vědomosti klientů bank, a tím zdokonalit jejich finanční gramotnost, což povede ke snížení rizika zneužití účtu. Pro vyřešení problému bude použito následující:

- Krok 1 – Zjištění úrovně povědomí o rizicích spojených s vedením bankovního účtu za pomocí dotazníku.
- Krok 2 – Kategorizace rizik spojených se vedením bankovního účtu.
- Krok 3 – Zpracování dotazníků.
- Krok 4 - Návrhy, jak se konkrétním rizikům bránit, jak je snížit.

3 Rešeršní studie

V rešeršní studii bylo zpracováno šetření dostupné literatury zabývajících se riziky v bankovnictví. Protože daná problematika nebyla v oblasti bankovnictví zpracována, lze tuto práci považovat za přínos v tomto směru, jedná se o zcela původní práci. V jednotlivých literárních zdrojích bylo následně vyhledáno zpracování této problematiky, které bylo následně použito.

3.1 Banky

Marvanová, Houda a kolektiv (1995) uvádí, že mluvíme-li o bance, máme obvykle na mysli banku obchodní, tzn. banku, která slouží tržním subjektům (výrobní a terciární sféře, respektive obyvatelstvu). Vedle obchodních bank existují samozřejmě i jiné banky, především centrální banka (cedulová, emisní), různé typy specializovaných bank, např. garanční, hypoteční, konsolidační, rozvojové apod. Zvláštní skupinu tvoří spořitelny, které většinou nedisponují plnou licencí univerzální banky.

Obchodní banka univerzálního typu se účastní hospodářského života v tržní ekonomice především těmito aktivitami:

- Vede účty a přijímá termínové vklady v domácí měně i v měnách cizích.
- Poskytuje různé druhy úvěrů, které se liší podle typu zajištění, způsobu čerpání, účelu poskytnutí, zdrojů, z kterých jsou čerpány, a podle délky úvěrovaného období.
- Provádí tuzemský a zahraniční platební styk prostřednictvím sítě „loro" účtů a „nostro" účtů (účtů cizích bank vedených „u sebe" a „svých" účtů vedených u jiných bank).
- Přijímá a vystavuje všechny druhy platebních a zajišťovacích instrumentů, jako jsou dokumentární inkasa, dokumentární akreditivy, směnky a jejich avalizace, všechny typy šeků, platební karty atd.
- Provádí financování prostřednictvím odkupu různých druhů pohledávek svých klientů, respektive odkupem dokumentů tyto pohledávky zajišťujících.
- Zajišťuje pro své klienty emisi a obchodování s cennými papíry, provádí operace na finančních trzích, devizově-arbitrážní a zajišťovací operace v cizích měnách.
- Provádí směnárenské a přepážkové operace pro stálé i příležitostné klienty. [3]

3.2 Bankovní služby

Máče (2006) uvádí, že mezi základní služby, které poskytují banky svým klientům, patří realizace platebního styku, tedy hotovostní a bezhotovostní přesuny peněžních

prostředků mezi jednotlivými subjekty hospodářského života – fyzickými i právnickými osobami, a to jak v rámci jednoho státu, tak i v zahraničí. [4]

3.2.1 Bankovní pojmy

Česká bankovní asociace (2017) vytvořila spotřebitelský slovníček, který dává spotřebiteli potřebné informace k používání bankovního účtu. Pro účely této diplomové práce bude použit pouze jejich výčet.

- Bankomat - peněžní výdajový automat, který slouží především k výplatě hotovosti v bankovkách pomocí platební karty či bankomatové karty.
    - *Další používaná označení:* ATM; Automatic Teller Machine
- Bezhotovostní operace - operace uskutečňovaná bez použití fyzických peněz (hotovosti) prostřednictvím bankovních převodů a dalších účetních operací.
    - *Další používaná označení:* Wire Transfer; Noncash Transfer; Cashless Transfer
- Běžný účet - bankovní účet, na kterém má klient uloženy peníze, které si může kdykoli vybrat nebo vložit další (s ohledem na podmínky stanovené bankou). Vklady a výběry peněžních prostředků z běžného účtu může klient uskutečňovat různými způsoby, například v hotovosti či pomocí bezhotovostních převodů z jiných účtů nebo na jiné účty (např. výplaty mzdy od zaměstnavatele či platby za poskytované služby).
    - *Další používaná označení:* Current Account
- Internetové bankovnictví - služba, která klientovi umožňuje komunikaci s bankou (včetně zadávání příkazů) pomocí internetu - nepotřebuje instalovat žádné speciální programy, postačí mu pouze internetové připojení.
    - *Další používaná označení:* Internet Banking
- Mobilní bankovnictví - jedna z možností využití přímého elektronického bankovnictví. Klient ke komunikaci s bankou (včetně zadávání platebních příkazů) používá GSM instalaci v mobilním telefonu (např. SIM toolkit) - oproti běžnému telefonnímu bankovnictví poskytuje vyšší míru ochrany klienta.
    - *Další používaná označení:* GSM Banking
- PIN - osobní identifikační číslo pro autorizaci transakcí (prováděných např. prostřednictvím platební karty, internetu)
    - *Další používaná označení:* Personal Identification Number
- Platební karta - karta, s jejíž pomocí lze platit za zboží a služby u většiny prodejců a vybírat hotovost v bankomatech, případně využívat jiné služby, které bankomat nabízí (např. dobíjení kreditů na mobilních telefonech).
    - *Další používaná označení:* Payment Card
- Telefonní bankovnictví - služba, která klientovi umožňuje komunikaci s bankou prostřednictvím telefonického spojení. Této služby lze využívat standardním způsobem, anebo prostřednictvím odpovídající instalace v

mobilním telefonu (např. sítě GSM), která zabezpečuje vyšší míru ochrany klienta (někdy též GSM Banking).

- *Další používaná označení:* Phone Banking [5]

3.2.2 Technologické pojmy

Mobilní aplikace

Viswanathan (2016) na webových stránkách Lifewire.com vysvětluje, že mobilní aplikace jsou vytvořené pro malá kapesní zařízení, jako jsou mobilní telefony, smartphony, PDA a další. Mobilní aplikace může být předem nahrána na kapesním zařízení nebo může být uživatelem přímo stažená z App Store nebo internetu. Všechny výše uvedené možnosti můžete najít jak na mobilních telefonech nebo smartphonech. Nejoblíbenější smartphone platformy, které podporují mobilní aplikace jsou Android, iOS, Windows Phone a BlackBerry. [6]

Touch ID

Chell, Erasmus, Colley a Whitehouse (2015) popisují, že Touch ID je technologie založená na rozpoznávání uživatele pomocí otisků prstů, která byla představena s iPhonem 5S. Funguje na principu stisknutí takzvaného „Home button", které se nachází přímo na mobilním telefonu. Touch ID senzor umožňuje uživateli alternativní verzi autentizace a následného přístupu do zařízení bez zadávání přístupového kódu. Umožňuje schvalování nákupů v App Store a iBooks a s verzí iOS8 umožňuje používat senzor i dalším stranám. [7]

Near Field Communication

Coskun, Ok a Ozdenizci (2012) dodávají, že Near Field Communication, dále jako NFC, je současně rozvíjející se, a přesto slibné pole působnosti, které bude mít enormní dopad na finanční ekosystémy stejně jako mobilní technologie během několik málo let. NFC je bezdrátová komunikační technologie s krátkým dosahem, která potenciálně usnadňuje používání mobilního telefonu miliardou lidí po celém světě. Nabízí enormní počet možností, jak jej využít, od kreditních karet až po debetní karty, věrnostní karty, klíče od auta, přístupové hotelové klíče, kancelářské klíče nebo klíče od domu, eventuálně zahrnuje všechny tyto možnosti do jednoho mobilního telefonu. [8]

3.2.3 Bezpečnost v internetovém bankovnictví

Česká národní banka vydala upozornění týkající se právě rizik spojených s využíváním elektronického bankovnictví. Pro přiblížení bylo vybráno pouze pár důležitých bodů, více o upozornění je možné se dočíst na webových stránkách výše

zmíněné České národní banky. Česká národní banka (2017) doporučuje věnovat pozornost následujícím skutečnostem:

- Vybavení zařízení používaného pro obsluhu bankovního účtu (aktualizovaný operační systém; aktualizovaný internetový prohlížeč; funkční a zapnutý antivirový program).
- Další doporučení v souvislosti se zařízením používaným k obsluze bankovního účtu (instalace pouze programů z důvěryhodných zdrojů; nepoužívat k obsluze bankovního účtu mobilní zařízení, u kterého byly provedeny změny nastavení tzv. „jailbreak" a „root"; mít zařízení pod trvalou kontrolou a využívat zámek obrazovky; používat výlučně důvěryhodné a řádně zabezpečené zařízení).
- Doporučení spojené s přihlášením a prokázáním totožnosti klienta.
- Zásady spojené s vylákáváním přihlašovacích informací.
- Další doporučení snižující riziko odcizení finančních prostředků. [25]

Výhodám a nevýhodám elektronického (internetového) bankovnictví se věnuje i Jiří Rousek a Tomáš Komínek (2007) ve své seminární práci s názvem „Rizika elektronického bankovnictví". Mezi výhody řadí například ušetřený čas pro klienta možnost komunikovat s bankou z různých míst. Mezi nevýhody patří nutnost přístupu k příslušnému elektronickému komunikačnímu kanálu a někdy též vlastnictví speciálního elektronického zařízení. Samozřejmostí také musí být znalost zacházení s tímto komunikačním kanálem, případně zařízením. [26]

4 Systémový přístup k rizikům v bankovnictví

V této části byla provedena analýza předmětu zájmu, tedy rizika v bankovnictví.

4.1.1 Historie rizika

Janíček, Marek a kolektiv (2013) uvádí, že riziko je historický výraz, pocházející údajně ze 17. století, kdy se objevil v souvislosti s lodní plavbou. V italštině „risico" označuje úskalí, kterému se musí plavci na moři vyhýbat. Následně se tímto pojmem vyjadřovalo „vystavení nepříznivým okolnostem". Starší encyklopedie uvádějí, že se jedná o odvahu či nebezpečí, případně, že „riskovat" znamená odvážit se něčeho. [9]

4.1.2 Riziko

Tichý (2006) uvádí, že názvem „riziko" se označují kvalitativně dosti rozdílné, byť velice příbuzné pojmy. Ukazuje se, že při hledání definice rizika jde o sémantický problém, který není univerzálně řešitelný. Záleží velice na odvětví, oboru a problematice, co se pod tímto názvem rozumí; záleží koneckonců i na jazyku, ve kterém se o riziku hovoří nebo píše (v češtině má „riziko" negativní odstín). Existují skupiny definic technický, ekonomických a sociálních. V technické a ekonomické literatuře se nejčastěji pak setkáváme s definicí rizika, která jej vymezuje jako pravděpodobnou hodnotu ztráty vzniklé nositeli, popř. příjemci rizika, realizací scénáře nebezpečí, vyjádřená v peněžních nebo jiných jednotkách. [10]

Smejkal a Rais (2013) dodávají, že pojem „riziko" tedy navazuje na filozofické kategorie, jakými jsou nutnost a nahodilost. Je podmíněn nahodilostí jako formou projevu nutnosti, což znamená, že zdrojem je objekt a jde o ontologický aspekt pojmu, jednak je podmíněn neúplností zobrazení reálných procesů v lidském vědomí – zdrojem je v tomto případě subjekt a jedná se o gnozeologický aspekt pojmu. [11]

4.1.3 Riziko, nejistota a nebezpečí

Pro úplnost je nezbytné rozlišovat pojmy riziko, nejistota a nebezpečí. Hnilica a Fotr (2009) vysvětlují, že riziko je vždy spojeno s určitou akcí, aktivitou či projektem s nejistými výsledky, přičemž tyto výsledky ovlivňují (často finanční) situaci subjektu, který akci realizuje. Např. neúspěch určitého projektu může vést ke vzniku hospodářské ztráty, problémům s peněžními toky, dokonce až k ohrožení existence podniku, s čímž jsou úzce spojeny i dopady na manažery odpovědné za přijetí realizaci tohoto projektu (počínaje finančními postihy, poškozením reputace, ztrátou pozice a konče až propuštěním). Na druhé straně úspěch projektu může posílit konkurenceschopnost podniku, zlepšit jeho hospodářské výsledky, tentokrát s příznivými dopady na manažery (finanční ohodnocení, povýšení aj.) Nejistota je pak spojena především se neschopností spolehlivého odhadu budoucího vývoje těchto faktorů (faktorů rizika) ovlivňujících výsledky aktivit, resp. projektů (vývoj

poptávky, prodejních cen, nákupních cen materiálů a energií, měnových kurzů, technologických změn aj.) Nejistota budoucích hodnot faktorů rizika se pak promítá do nejistoty výsledků realizovaných podnikatelských aktivit či projektů a je příčinou jejich rizikovosti. Pojetí rizika a nejistoty může být zčásti závislé na oboru, ve kterém se s nimi pracuje. Např. v teorii rozhodování se rozhodování za rizika chápe jako rozhodování, kdy jsou známy stavy světa i jejich pravděpodobnosti, přičemž v případě, že tyto pravděpodobnosti známy nejsou, jde o rozhodování za nejistoty. Omezenou spolehlivost stanovení budoucích hodnot faktorů rizika nepříznivě ovlivňuje více aspektů, k nimž patří především:

- Nedostatek informací a nedostatečné poznání procesů, které generují faktory rizika a nejistoty.
- Použití nevhodných zdrojů informací a neověřených, resp. nespolehlivých dat.
- Uplatnění nevhodných metod odhadu budoucího vývoje faktorů rizika a nejistoty.
- Náhodný (stochastický) charakter procesů, jejichž výsledkem jsou hodnoty rizikových faktorů.

Z výše uvedeného je zřejmé, že nejistotu (nespolehlivost) odhadu vývoje faktorů rizika a nejistoty lze snížit (např. lepším poznáním procesů generujících tyto faktory, lepším informačním vybavením, užitím variantních a spolehlivějších zdrojů dat, uplatněním vhodnějších metod prognózování aj.), ale nelze ji zcela odstranit vzhledem k náhodné povaze procesů generujících rizikové faktory. [12]

Janíček, Marek a kolektiv (2013) ve své publikaci pojednávají o rozdílnost pojmů rizika a nebezpečí. Riziko je pravděpodobnost vzniku nestandardního stavu konkrétní entity v daném čase a prostoru. Nebezpečí je aktivovaná schopnost (přírodou, člověkem, strojem) zdroje nebezpečí, která pak na rizikové entitě způsobí negativní jev. [9]

4.1.4 Klasifikace rizik

Fotr a Hnilica (2009) člení rizika na:

- Podnikatelské a čisté; podnikatelské riziko (Business Risk) má již zmíněnou pozitivní a negativní stránku, přičemž čisté riziko (Pure Risk) má pouze stránku negativní, tj. existuje zde nebezpečí vzniku nepříznivých situací, resp. nepříznivých odchylek od žádoucího stavu, za který se považuje uchování majetku, zdraví a lidských životů. Čistá rizika se obvykle vztahují ke ztrátám a škodám na majetku organizací a jednotlivců, poškození zdraví, resp. ztrátám života jednotlivců a členů organizačních jednotek vyvolaných přírodními jevy (např.: povodně, požáry, zemětřesení aj.), technickými systémy a jejich

selháním (např. havárie výrobních zařízení) a jednáním lidí (krádeže a zpronevěry, stávky aj.).

- Systematické a nesystematické; systematické riziko je riziko vyvolané společnými faktory a postihující v různé míře všechny hospodářské jednotky, resp. oblasti podnikatelské činnosti. Zdrojem systematického rizika jsou např. změny peněžní a rozpočtové politiky, změny daňového zákonodárství, celkové změny trhu (konjunkturální cykly, změny cen základních surovin a energií aj.). Protože systematické riziko závisí do značné míry na celkovém vývoji trhu, označuje se jako riziko tržní. Toto riziko vzhledem ke společnému charakteru nelze snižovat diverzifikací, a proto se označuje též jako nediverzifikovatelné. Riziko nesystematické (jedinečné, specifické) je riziko, které je specifické pro jednotlivé firmy, resp. jejich aktivity. Zdrojem takového rizika může být např. odchod klíčových pracovníků firmy, selhání významného subdodavatele, vstup nového konkurenta na trh, havárie výrobního zařízení aj. Vzhledem ke svému charakteru představují systematická rizika obvykle rizika makroekonomická, rizika nesystematická pak rizika mikroekonomická.
- Vnitřní a vnější; vnitřní rizika jsou rizika, která se vztahují k faktorům uvnitř firmy, (může jít např. o rizika výzkumně-vývojová, resp. technicko-technologická spojená s výzkumem a vývojem nových výrobků a technologií, rizika selhání pracovníků aj.). Vnější rizika se vztahují k podnikatelskému okolí, ve kterém firma podniká. Jejich zdrojem jsou externí faktory, které se člení na makroekonomické (v podobě ekonomického, sociálního, technicko-technologického a ekologického makrookolí) a mikroekonomické (konkurence, dodavatelé, odběratelé aj.).
- Ovlivnitelné a neovlivnitelné; toto členění rizik souvisí s možností manažera či firmy působit na příčiny jejich vzniku. Jako ovlivnitelné se chápe riziko, které lze eliminovat, resp. oslabit opatřením orientovaným na jeho příčiny, a to ve smyslu eliminace, resp. snížení pravděpodobnosti vzniku či rozsahu možných nepříznivých situací (např. zvýšením kvalifikace pracovníků výzkumu a vývoje, zlepšením jejich přístrojového vybavení apod. lze snížit rizika výzkumu a vývoje nových výrobků a technologií). U neovlivnitelného rizika nemáme možnost působit na jeho příčiny (např. nepříznivá změna měnového kurzu, povodeň aj.), ale můžeme přijmout opatření snižující nepříznivé následky těchto rizik (např. formou zajištění, pojištění). Vnitřní rizika jsou spíše ovlivnitelná, vnější rizika většinou neovlivnitelná.
- Primární a sekundární; sekundární riziko je vyvoláno přijetím určitého opatření na snížení primárního rizika tvořeného všemi výše uvedenými faktory. Příkladem sekundárního rizika může být riziko spojené s existencí odlišné podnikové kultury při vytvoření společného podniku se zahraničním partnerem, která může být příčinou jeho neúspěchu (přitom tvorba

společného podniku byla opatřením orientovaným na oslabení rizika primárního, např. vstupu na zahraniční trh).

- Ve fázi přípravy, realizace a provozu firemních projektů; rizika ve fázi přípravy a realizace projektu představující všechny druhy rizik, která ohrožují splnění termínu dokončení projektu, dodržení rozpočtu a kvalitu projektu (např. nebezpečí nedostatků projektového řešení, rizika selhání subdodavatelů stavební a strojní části projektu, nepříznivá změna měnového kurzu ovlivňující cenu dovážené technologie aj.). Rizika ve fázi provozu představují všechny rizikové faktory ovlivňující hospodářské výsledky fungování projektu (např. vzrůst cen surovin, materiálů a energie, pokles poptávky, nedosažení projektované kapacity nezvládnutím technologického procesu aj.).

Významné a značně bohaté je členění rizik podle jejich věcné náplně. Z tohoto hlediska se obvykle rozlišují rizika:

- Technicko-technologická, spojená s aplikací výsledků vědecko-technického rozvoje a vedoucí k neúspěchu vývoje nových výrobků a technologií, nezvládnutí technologického procesu spojeného s poklesem výrobní kapacity aj. (Tato rizika se mohou projevovat též objevením nových produktů a postupů, které vedou k morálnímu zastarání technologií.)
- Výrobní, která mají často charakter omezenosti, resp. nedostatku zdrojů různé povahy (surovin, materiálů, energií, pracovních sil určité kvalifikace), které mohou ohrozit průběhu výrobního procesu a jeho výsledky. Příčinou některých výrobních rizik spojených s omezeností zdrojů mohou být nedostatky a poruchy na straně dodavatelů (rizika dodavatelská). Mezi výrobní rizika je možné zařadit i rizika projevující se např. nespolehlivostí a výpadky výrobních zařízení spojených s omezením dodávky produktů či služeb, vzrůstem nákladů a opravy a údržbu aj. Tato rizika se někdy označují jako provozní rizika nebo také jako operační rizika. [12]

4.1.5 Identifikace rizik

Fotr a Hnilica (2014) se shodují na tom, že cílem identifikace rizik je dospět k vyčerpávajícímu souboru rizikových faktorů, které by mohly (nejen negativně, ale také pozitivně) ovlivnit hospodářské či jiné výsledky firmy, hodnotu jejích určitých aktiv nebo míru úspěšnosti připravovaných, resp. realizovaných investičních projektů. Proces identifikace rizik má několik stránek, přičemž mezi nejdůležitější patří vhodná dekompozice objektu analýzy rizika, vlastní náplň procesu identifikace, používané metody a nástroje podporující identifikaci, informační zdroje i subjekty podílející se na identifikaci.

Nástroje identifikace a informační zdroje

- Kontrolní seznamy (check listy), resp. katalogy (registry) rizik, které poskytují vyčerpávající přehled potenciálních rizikových faktorů firmy či jejích aktivit. Uplatnění seznamů snižuje nebezpečí opomenutí některých rizik.
- Pohovory s experty a skupinové diskuse. Tyto diskuse mohou mít formu brainstormingových schůzek, kdy skupinu tvoří pracovníci firmy, externí experti aj. Schůzku řídí moderátor, nejlépe rizikový analytik, který zabezpečuje, aby se každý mohl vyjádřit bez ohledu na své postavení, podněcuje diskusi, sumarizuje výsledky a směřuje debatu k závěru; v průběhu diskuse panuje zákaz kritiky vyjadřovaných názorů. Týmová práce podněcuje kreativitu, která je podstatná pro identifikaci rizik a umožňuje sdílení informací a zkušeností.
- Nástroje strategické analýzy podnikatelského prostředí (SWOT analýza, PEST analýza, Porterův model pěti sil aj.), které podporují především identifikaci externích rizik.
- Kognitivní (myšlenkové) mapy, jež představují grafický nástroj zobrazení jednotlivých faktorů rizika a jejich vzájemných vazeb. Rizikové faktory se zapisují na list papíru a orientovanými spojnicemi se zobrazují jejich vzájemné vazby. Spojnice vychází z faktoru rizika na straně příčiny a šipka směřuje k faktoru na straně dopadu rizika.

Jako zdroje informací pro identifikaci faktorů rizika může sloužit především informační a znalostní vybavení expertů z oblastí, ke kterým se jednotlivé faktory vztahují, výstupy strukturovaných rozhovorů a dotazníků, lokální či zahraniční zkušenosti osobní či firemní povahy, výstupy, resp. doporučení externích auditorů, výsledky finančního controllingu a interního auditu, příprava podnikatelského plánu firmy, periodické analýzy firemních výsledků, výstupy monitorovacích systémů či systémů včasného varování a v neposlední řadě poznatky a zkušenosti z realizace významných projektů. [13]

4.1.6 Metody analýzy rizik

Smejkal a Rais (2013) ve své publikaci konstatují, že způsob vyjádření veličin, s nimiž se v analýze rizik pracuje, lze použít jako základní hledisko pro rozdělení těchto metod. Existují přitom dva základní přístupy k jejímu řešení: kvantitativní a kvalitativní metody vyjádření veličin analýzy rizik. V analýze se používá buď jeden z těchto dvou přístupů, nebo jejich kombinace.

Kvalitativní metody

Kvalitativní metody jsou postaveny na popisu závažnosti potenciálního dopadu a na pravděpodobnosti, že daná událost nastane.

Vyznačují se tím, že rizika jsou vyjádřena v určitém rozsahu (například jsou obodována <1 až 10> nebo určena pravděpodobností <0; 1> nebo slovně <malé, střední, velké> apod.) Úroveň je obvykle určována kvalifikovaným odhadem. Kvalitativní metody jsou jednodušší a rychlejší, ale více subjektivní. Obvykle přinášejí problémy v oblasti zvládání rizik, při posuzování přijatelnosti finančních nákladů nutných k eliminaci hrozby, která může být kvalitativní metodou charakterizována třeba jako „velká až kritická". Tím, že chybí jednoznačně finanční vyjádření, se kontrola efektivnosti nákladů znesnadňuje. Tento typ analýzy se s výhodou využívá v případech:

- Upřesnění postupů při detailní analýze rizik.
- Nedostatečné kvality či kvantity získaných číselných údajů pro jejich využití v kvantitativních metodách.

Kvantitativní metody

Kvantitativní metody jsou založeny na matematickém výpočtu rizika z frekvence výskytu hrozby a jejího dopadu. Používají číselné ocenění jak v případě pravděpodobnosti vzniku události (či lépe řečeno incidentu), tak i při ocenění dopadu dané události. Vyjadřují dopad obvykle ve finančních termínech, například „tisíce Kč". Nejčastěji je riziko vyjádřeno ve formě roční předpokládané ztráty (annualized loss expectancy – ALE), která je vyjádřena finanční částkou. Kvantitativní metody jsou více exaktní než kvalitativní; jejich provedení sice vyžaduje více času a úsilí, poskytují však finanční vyjádření rizik, které je pro jejich zvládání výhodnější.

Nevýhodou kvantitativních metod je kromě jejich náročnosti na provedení a zpracování výsledků často vysoce formalizovaný postup, jenž může vést k tomu, že nebudou postihnuta specifika posuzovaného subjektu, která mohou vést k jeho vysoké zranitelnosti, a to z důvodů „zahlcení" hodnotitele značným objemem formálně strukturovaných dat. (Dalo by se vyjádřit rčením „kvůli stromům není vidět les".) Kvalita výsledků těchto metod úzce souvisí s relevantností získaných údajů.

Kombinované metody

Kombinované metody vycházejí z číselných údajů. Cíl je však díky kvalitativnímu hodnocení ve větším přiblížení se realitě oproti předpokladům, ze kterých vycházejí kvantitativní metody. Je ovšem třeba mít na zřeteli, že údaje použité v kvalitativních

metodách nemusí vždy odrážet přímo pravděpodobnost události či výši jejího dopadu, ale mohou být ovlivněny měřítkem stupnice, která je v konkrétní metodě použita. [11]

4.1.7 Měření rizika

Fotr a Hnilica (2014) uvádí, že základem měření rizika je stanovení jeho číselných charakteristik v podobě charakteristik variability (pravděpodobnost ztráty, rozptyl či směrodatná odchylka) zvoleného kritéria, např. hodnoty firmy, kritérií hodnocení investičních projektů jako čistá současná hodnota aj. To však vyžaduje jednak kvantitativní charakter veličiny (kritéria), vzhledem ke kterému se riziko určuje, jednak znalost jeho rozdělení pravděpodobnosti. V opačném případě není číselné měření rizika možné, ale lze uplatnit určité kvalitativní (verbální) charakteristiky.

Číselné charakteristiky rizika

Měřením rizika budeme rozumět číselné stanovení velikosti rizika určité podnikatelské aktivity (např. investičního projektu), firemního aktiva (např. finančních investic) či firmy jako celku. Přitom je třeba si uvědomit, že toto riziko lze vyjadřovat vždy pouze vzhledem k určitému kritériu kvantitativní povahy, které zobrazuje číselné výsledky této aktivity a slouží k jejímu hodnocení. Tímto kritériem může být např. zisk firmy za určité období, rentabilita jejího kapitálu; u investičních projektů jejich čistá hodnota, vnitřní výnosové procento či doba úhrady; u finančních investic pak jejich tržní hodnota k určitému datu aj.

Jakožto číselné charakteristiky rizika mohou sloužit:

- Pravděpodobnost nedosažení (případně překročení) určité hodnoty kritéria.
- Statistické charakteristiky variability kritéria, zahrnující rozptyl, směrodatnou odchylku a variační koeficient.
- Hodnoty kritéria, které budou překročeny (či nedosaženy) se zvolenou pravděpodobností.

Kvalitativní charakteristiky rizika

Jak je z předchozího textu zřejmé, nelze dospět k číselným charakteristikám rizika bez znalosti rozdělení pravděpodobnosti kritéria (veličiny), vzhledem ke kterému se riziko vyjadřuje. Pokud není toto rozdělení k dispozici, lže použít k popisu rizika kvalitativních (verbálních) charakteristik v podobě slovních popisů. Např. velikost rizika určitého investičního projektu můžeme vyjádřit pomocí některého hodnocení ze stupnice uvedené v tabulce.

Tab. 1 Stupnice kvalitativního vyjádření rizika

Stupeň	Slovní charakteristika rizika
1	Velice malé riziko
2	Malé riziko
3	Střední riziko
4	Vysoké riziko
5	Zvláště vysoké riziko

Zdroj: Fotr, J., Hnilica, J., 2014. [13]

Je zřejmé, že stupnice po kvalitativní měření rizika uvedená v tabulce 1 není jediná, ale může být buď detailní s větším počtem stupňů, nebo stručná s menším počtem stupňů. Zařazení určitého objektu, např. investičního projektu do některého ze stupňů rizika, by pak mělo být založeno především na zvažování:

- Rizik, resp. faktorů rizika, které by mohly ohrozit úspěšnost projektu (čím je počet těchto faktorů větší a čím méně je lze ovlivnit, tím větší může být i riziko projektu).
- Možných dopadů výskytu těchto rizik na úspěšnost projektu (někdy lze tyto dopady, např. velikost ztráty v případě výskytu určitého rizika, stanovit číselně, někdy to možné není, a proto je třeba opírat se např. o expertní odhady pravděpodobných rozsahů těchto dopadů, implicitní zvažování účinků rizik na projekt, manažery aj.)

Na rozdíl od kvantitativního měření rizika, které je odděleno od jeho hodnocení, se při užití kvalitativních charakteristik prolíná měření rizika s jeho hodnocením. Při tomto hodnocení má pak velkou váhu organizační kontext (např. rozsah projektu a možné dopady jeho neúspěchu na podnik, kdy realizace malého, i když vysoce rizikového projektu jej nemůže ohrozit) i to, jak se k riziku staví manažeři, kteří rozhodují o přijetí či zamítnutí projektu.

4.1.8 Hodnocení rizika

Výsledky analýzy rizika poskytují podklady pro posouzení, zda riziko spojené s určitým objektem (firmou, složkami jejich aktiv, rozvojovými plány či investičními projekty) je přijatelné či nepřijatelné. Závěr o přijatelnosti rizika určité aktivity, resp. projektu (např. fúze či akvizice, zavedení nového produktu či technologie aj.) ovlivňuje především riziková kapacita firmy a velikost rizika, kterou je firma ochotna tolerovat. Riziková kapacita (Risk Capacity) se vyjadřuje obvykle jako nejvyšší finanční ztráta, kterou je firma schopna přežít, tj. taková velikost ztráty, která ještě neovlivní výrazně existenci firmy. Výše rizikové kapacity závisí především na velikosti kapitálu

firmy, jeho struktuře a schopnosti získat další zdroje financování. Je zřejmé, že riziková kapacita firmy je tím větší, čím větší je:

- Její celkový kapitál.
- Podíl vlastního kapitálu na celkovém kapitálu, který ovlivňuje finanční stabilitu firmy.
- Schopnost získat dodatečné zdroje financování – tuto schopnost ovlivňuje především posouzení její bonity, resp. finančního zdraví, vyjádřené ratingem od některých z renomovaných ratingových agentur (Moody's, Standard & Poor aj.)

Velikost přijatelného, resp. tolerovaného rizika (Risk Appetite) představuje takovou výši ztráty, kterou je organizace ochotna přijmout v rámci své rizikové kapacity. Rozhodnutí o velikosti přijatelného rizika patří mezi významná strategická rozhodnutí firmy a závisí především na:

- Požadavcích a očekáváních stakeholderů (akcionářů, věřitelů, regulátorů, finančních institucí, ratingových agentur aj.).
- Postoji managementu k riziku, tj. zda převládá spíše averze k riziku, či ochota přijímat riziko.

Postoj k riziku

Rozhodovatel (manažer, podnikatel) může mít k riziku buď averzi, sklon nebo neutrální postoj. V oblasti investičního rozhodování:

- Rozhodovatel s averzí k riziku se snaží vyhnout volbě značně rizikových projektů a vyhledává málo rizikové projekty, které s vysokou pravděpodobností vedou k dosažení výsledků, které jsou pro ně přijatelné.
- Rozhodovatel se sklonem k riziku naopak vyhledává značně rizikové projekty (které mají naději na dosažení zvláště dobrých výsledků, ale jsou spojeny i s vyšším nebezpečím špatných výsledků, resp. ztrát) a preferuje je před projekty málo rizikovými.
- U rozhodovatele s neutrálním postojem k riziku jsou averze a sklon k riziku ve vzájemné rovnováze.

Definice postoje rozhodovatele k riziku je založena na jeho chování v situaci, kdy má možnost volby mezi dvěma projekty, které jsou potenciálně stejně výnosné (střední hodnota výnosového kritéria, např. zisku, je u obou projektů stejná), avšak liší se svým rizikem.

Jestliže první projekt má vyšší riziko, pak rozhodovatel:

- S averzí k riziku dá přednost druhému projektu s menším rizikem před prvním, rizikovějším projektem.
- Se sklonem k riziku preferuje první rizikovější projekt před druhým, méně rizikovým projektem.
- S neutrálním postojem k riziku hodnotí oba projekty stejně vysoko.

Určitý nástroj umožňující kvantitativní vyjádření postoje subjektu k riziku představuje funkce užitku za rizika. Postoj rozhodovatele, resp. manažera k riziku závisí na větším počtu faktorů, z nichž k nejvýznamnějším patří jeho osobnostní charakteristiky a založení, dřívější zkušenosti (úspěšnost či neúspěšnost předchozích rizikových rozhodnutí, kdy minulá úspěšnost podporuje ochotu jít do rizika a naopak neúspěšnost posiluje averzi k riziku) a systém řízení firmy (především motivační systém, kdy důraz na krátkodobé výsledky a malá tolerance dílčích neúspěchů zvyšuje averzi k riziku a naopak zaměření spíše na dlouhodobější výsledky s tolerováním dílčích neúspěchů posiluje ochotu vzít na sebe riziko). Z empirických výzkumů plyne, že u manažerů v hospodářské praxi převládá averze k riziku. [13]

4.1.9 Řízení rizik

Smejkal a Rais (2013) definují řízení rizik jako proces, při němž se subjekt řízení snaží zamezit působení již existujících i budoucích faktorů a navrhuje řešení, která pomáhají eliminovat účinek nežádoucích vlivů a naopak umožňují využít příležitostí působení pozitivních vlivů. Součástí procesu řízení rizik je rozhodovací proces, vycházející z analýzy rizika. [11]

4.1.10 Prevence rizik

Fotr a kolektiv (2012) konstatují, že smyslem preventivních opatření je eliminovat, resp. alespoň oslabit příčiny vzniku rizik, tj. předejít výskytu rizikových situací, resp. Alespoň snížit pravděpodobnost jejich výskytu. Jde tedy o určitou prevenci rizika. Je zřejmé, že opatření tohoto charakteru jsou možná především u rizik interních, která jsou spíše ovlivnitelná než u rizik externích. Jako příklady opatření této povahy lze uvést:

- Uplatňování nástrojů řízení, jako jsou systémy řízení jakosti, systémy environmentálního managementu, systémy protipožární prevence, systémy prevence bezpečnostních rizik ohrožujících lidi a majetek aj.
- Změny procesů (postupů) vedoucích k eliminaci či oslabení vzniku rizikových událostí.
- Kvalita informace a těsnost styku se zákazníky, umožňující snížení tržních rizik;
- Kvalitní výběrová řízení zabezpečující pečlivý výběr dodavatelů.

- Vertikální integrace, oslabující rizika spojená s cenovým vývojem či omezenou dostupností určitých polotovarů či komponent tím, že se jejich nákup nahradí vlastní výrobou.
- Získávání dodatečných informací (pokud je nejistota vyvolána nedostatečným poznáním určitých procesů či objektů); příkladem mohou být analýzy trhu, získávání informací o konkurentech, obchodních partnerech aj. [14]

5 Rizika spojená s vedením bankovního účtu

Ne každý vlastník bankovního účtu si uvědomuje, že dokáže sám snižovat rizika, která se mohou v průběhu používání účtu vyskytnout. Tahle skutečnost může vyplývat z faktu, že finanční gramotnost je v České republice na velmi nízké úrovni. Ostatně jsou tato tvrzení založena na měření úrovně finanční gramotnosti dospělé populace České republiky, které provedlo Ministerstvo financí na konci roku 2015. Ministerstvo financí České republiky (2016) uvádí, že toto šetření se stalo součástí světového měření společně s dalšími desítkami zemí Organizace pro hospodářskou spolupráci a rozvoj (OECD). Výsledky tohoto měření lze sledovat přímo na stránkách Ministerstva financí. Mezi zásadní zjištění můžeme zařadit například fakt, že dvě třetiny dospělých se nechovají ekonomicky zodpovědně, 57 % domácností nesestavuje rodinný rozpočet, 37 % respondentů si nedokáže představit, jak by řešili ztrátu hlavního příjmu jejich domácnosti, aktivně nespoří 19 % dospělých a další. [1]

V další části této práce se budeme věnovat právě nejčastějším prohřeškům vlastníků účtů. Všechny poznatky byly získány z důvěryhodných zdrojů s patřičnou praxí v daném oboru.

5.1 Rizika přímo ovlivnitelná klientem

5.1.1 Rizika spojená s platbou platební kartou na internetu

Určitá část uživatelů bankovních účtů nevěnuje pozornost kvalitě a důvěryhodnosti webových stránek přes které chce uskutečnit obchod. V tomto případě máme na mysli webové stránky, které nejsou příliš známé, nejsou v povědomí uživatelů internetu, mají pochybný vzhled, jsou nedokončené a v neposlední řadě chtějí po potenciálním uživateli při vstupu číslo jeho platební karty. Na výše uvedených typech webových stránek odsouhlasí smluvní podmínky, které ne každý uživatel čte a následně při nákupu služby nebo výrobku zadají čísla svých platebních karet, která jsou následně použita pro strhávání pravidelných plateb v určitém intervalu. Zpravidla se jedná o denní, týdenní nebo měsíční intervaly. V tomto období je uživateli strhávána částka v určité výši. Částky se pohybují v rozmezí od 1 koruny až po několika tisícové částky. Snaha o zabezpečení karet je ze strany bank maximální, instituce při nákupech podporují takzvané 3D Secure. Jedná se o zabezpečení, které podporuje platby kartou na internetu, kdy se údaje o platební kartě k obchodníkovi nedostanou. Princip spočívá v odeslání potvrzovací SMS zprávy nebo e-mailu, který upozorní nakupujícího, že pro pokračování je nezbytné zadat kód, který byl odeslán právě formou SMS zprávy

nebo e-mailem. Banky v České republice se snaží s tímto systémem pracovat v co nejširším měřítku. Nemůže však obchodníka, zahraničního nebo českého, donutit ke spolupráci a propojení platební brány s tímto systémem.

Jak proti tomu bojovat?

Pro zvýšení bezpečí při používání platebních karet při nakupování po internetu, stačí, když si před nákupem majitel platební karty důkladně pročte obchodní podmínky. Mnohdy jsou v nich obsaženy informace, které mohou nakupujícího zarazit. Jedná se zejména o část, kde si například daná stránka nárokuje strhávat pravidelné měsíční platby v určité výši. Tomu se dá zabránit i pečlivou kontrolou a nastudováním recenzí webových stránek, z kterých majitel platební karty nakupuje. Dalším poznávacím znamením může být například podmínka, která donutí nakupujícího, aby při vstupu na webové stránky nejdříve zadal číslo své platební karty. Na těchto stránkách se nedoporučuje nic zadávat, jelikož to ve většině případů vede ke strhávání pravidelných plateb, o kterých majitel karty nemá kolikrát ani povědomí.

Pro zvýšení bezpečnosti lze doporučit nakupovat pouze na stránkách, které podporují 3D Secure. Jak bylo zmíněno výše, tento způsob placení neposílá informace o kartě konkrétnímu obchodníkovi, riziko zneužití karty se eliminuje. Zneužití platební karty je možné eliminovat i snížením limitu pro platbu na internetu na částku v hodnotě do 1000 korun nebo dle uvážení majitele karty. Pokud se bude pokoušet obchodník strhnout částku vyšší, limit jej nepustí.

5.1.2 Rizika spojená uchováváním a vlastnostmi PIN kódu

Velmi často si uživatelé bankovních účtů neuvědomují rizika spojená se zapisováním PIN kódu od karty na různá místa. Mezi nejčastější prohřešky patří zapsání kódu přímo na povrch konkrétní karty. Takový zápis je většinou proveden nesmazatelným a nesmyvatelným popisovačem. Z pohledu uživatele účtu se může jednat o zjednodušení práce s kartou. Nicméně se jedná o velmi nebezpečný a nepraktický způsob, jak se zbavit zodpovědnosti za bezpečí svého účtu. Tento způsob ulehčení je v dnešní době velice častý. Můžeme hovořit například o zvyšujícím se trendu užívání mobilních telefonů, které mohou vést ke zhoršení krátkodobé paměti nebo i k poruchám soustředění. Více se této problematice věnuje doktor Lee Hadlington, který publikoval ve své studii možné následky užívání „chytrých" mobilních telefonů v běžném životě. Podle deníku Independent (2015), který se o studii v jednom ze svých článků zmínil, vede časté používání mobilního telefonu k poruchám kognitivních schopností. Studie zmiňuje například i to, že uživatelé mobilního telefonu zapomínají, proč šli z jedné do druhé části svého domu.

Čím více používají mobilní telefon, tím hůře se soustředí. Na to může navazovat i myšlenka, že jsou lidé pohodlní, a proto se nesnaží si PIN kód pamatovat a píšou si jej do elektronických zařízení nebo přímo na kartu. [15]

Na to navazuje i další porušení bezpečnosti, jako již dříve zmíněné, zapisování PIN kódů do mobilního telefonu. Tento způsob je oblíbený hlavně mezi mladší generací, která je na mobilních telefonech a technologii jako takové, závislá. Bohužel je na tento způsob zábavy už v dnešní době naráženo spíše jako na závislost, která často může vést až ke ztrátě komunikace mezi lidmi a jejich vzájemnému odcizení. Nadměrné využívání mobilního telefonu jako prostředku pro surfování na internetu nebo i jinak v běžném životě, stejně jako zařízení pro uložení PIN kódu zvyšuje riziko, jak v oblasti zhoršení krátkodobé paměti, tak z pohledu navyšování rizik při využívání bankovního účtu.

Posledním, ne příliš častým případem, je vyrytí PIN kódu na konkrétní bankomat. Uživatel platební karty a konkrétního bankomatu spoléhá na anonymitu spojenou se zápisem na povrch bankomatu. Ne vždy je tento způsob „pamatování" PIN kódu tak bezpečný, jak si jeho majitel může myslet. Pokud by si kolemjdoucí všiml nápadné kontroly právě vyrytého PIN kódu, mohl by toho později zneužít.
V bankovní praxi se dále můžeme setkat s jednoduchými hesly, ať už k přihlášení do internetového bankovnictví, nebo jako forma PIN kódu. Co si pod pojmem jednoduchého hesla představit? Nejčastěji se jedná o data nebo roky narození, ať už vlastníků účtu nebo jejich nejbližších. Není tedy těžké kód uhodnout.

Jak proti tomu bojovat?

Zvolit si PIN kód, který nebude mít nic společného s osobními daty anebo si ponechat PIN kód předem určený bankou a pracovat na jeho zapamatování. Dále se vyhýbat elektronickému zápisu do mobilního nebo jiného zařízení.

5.1.3 Rizika spojená s internetovým bankovnictvím

Z měření Českého statistického úřadu (2016) vyplývá, že 45 % dospělé populace a 59 % uživatelů internetu používají internetové bankovnictví. Nesmíme opomenout, že internet je podniky dlouhodobě používán především k bankovním službám, v lednu 2015 ho k tomuto účelu využilo 93 % podniků s 10 a více zaměstnanci. [16] Z těchto důvodů je nezbytné soustředit se na další rizika, která jsou spojena s vedením bankovního účtu a jeho uživatele o tom informovat. Cílem internetového bankovnictví je, aby klient získal patřičný přehled o svých financích, a taky možnost s nimi pracovat. Protože se vzhled i struktura internetových bankovnictví u různých institucí liší, nelze říci, že všechna umožňují klientovi přenastavit například své limity na platební kartě. Banky, které neumožňují, aby si klient tyto položky přenastavil,

poskytují podporu v podobě telefonního bankovnictví nebo pomoc na pobočce dané banky. Přihlašovací údaje, které klient používá, jsou velmi citlivá data, která může znát pouze on. Ne každý uživatel se tímto řídí a své údaje sdílí se svými nejbližšími nebo i s kamarády, což zvyšuje riziko zneužití účtu. Bezpečnost je porušena i v případě, kdy s klient uloží údaje ve svém internetovém prohlížeči. Riziko se zvyšuje v okamžiku, kdy svůj počítač dává do servisu, zůstává permanentně přihlášen u nechráněného počítače nebo jej půjčí někomu jinému. Při práci s internetovým bankovnictví je doporučeno, aby jeho uživatel v době přihlášení byl fyzicky sám přítomen u bezpečného počítače a ihned se po vyřízení svých záležitostí odhlásil.

Na tohle téma úzce navazují další rizika, která jsou neovlivnitelná bankou a jen částečně ovlivněná klientem. Jedná se o takzvaný phishing. Pod tímto pojmem se skrývá úmyslné napadání účtů klientů bank. Phishing může být prováděn e-mailem nebo třeba i SMS zprávou. Text zprávy může, ale i nemusí, být napsán pravopisnou češtinou a obsahuje odkaz, který nabádá klienty bank, aby si díky němu změnili heslo do svého internetového bankovnictví, protože jejich účet může být v ohrožení. Pod touto záminkou se nic netušící klient proklikne na falešné stránky, kde zadá své přihlašovací údaje, díky kterým má útočník přístup k účtu klienta dané banky. Klient může snížit riziko pouze svojí obezřetností a náležité kontrole při zadávání názvu webové stránky do internetového prohlížeče. Dále si může pravost stránky ověřit příslušným certifikátem.

Jak proti tomu bojovat?

Neukládat si přihlašovací údaje do internetového prohlížeče ani do jiných aplikací. Nezapisovat si údaje ani elektronicky do mobilního či jiného zařízení a ani na papír. Své přihlašovací údaje nikomu v žádném případě nesdělovat. Pro přihlašování používat pouze zařízení, které je plně důvěryhodné a má funkční antivirový systém. Dále užívat pouze oficiální webové stránky, kontrolovat si překlep a záměnu písmen v příkazovém řádku, a také se ujistit o platném certifikátu, který stvrzuje věrohodnost stránek. V případě obdržení zprávy, která se může jevit jako podezřelá, nejdříve kontaktovat banku, s kterou znění zprávy konzultovat. Poté postupovat dle pokynů konkrétní banky.

Pokud klient ztratí své údaje neprodleně kontaktovat banku a okamžitě vzniklou situaci řešit.

5.1.4 Rizika spojená s platební kartou

Platební kartu využívá čím dál více obyvatelstva naší republiky, ostatně to potvrdil i průzkum České bankovní asociace. Česká bankovní asociace (2016) uvádí, že v posledních 10 letech roste oblíbenost platby kartou na úkor hotovosti.

Podíváme-li se na tento typ bezhotovostních transakcí, vidíme růst jak v jejich počtu (za 10 let téměř čtyřnásobný), tak v objemu (2, 3 krát vyšší). [2]

Avšak i při používání platební karty je nezbytná obezřetnost a dodržování bezpečnosti. Jedná se zejména o pravidlo, že platební kartu může užívat pouze její majitel. Tímto se však bohužel neřídí všichni uživatelé platebních karet. Dochází k zapůjčování karet mezi příbuznými, kamarády nebo partnery. Pokud po zapůjčení karty dojde ke zneužití, je složité zjistit, proč se tak stalo, protože kartu neměl majitel v ten moment pod kontrolou.

Jak situaci předejít?

Banky v České republice umožňují, aby majitel vydal ke svému účtu další platební kartu. Jedná se zpravidla o funkci, která se nazývá „držitel". Tento držitel bude mít kartu vedenou na své jméno, ale finance bude čerpat z účtu majitele, který mu kartu vydal. Tímto způsobem se dá eliminovat riziko, že bude karta po zapůjčení zneužita, protože ji bude mít majitel účtu, i banka, neustále pod kontrolou.

5.1.5 Rizika spojená s použitím mobilní aplikace

Mobilní aplikace jsou hitem moderní doby. Ostatně průzkum společnosti VISA je toho důkazem. VISA (2016) uvádí, že v současnosti používá mobilní zařízení k placení 54 % dotazovaných, zatímco před rokem takto platilo za každodenní výdaje a služby jen 18 % z nich. Studie, ve které odpovídalo více než 36 tisíc respondentů z 19 zemí, odhaluje, jak dramaticky se přijímání digitálních plateb za posledních 12 měsíců posunulo. Před rokem odpovědělo 38 % osob, že mobilní zařízení k provedení platby nikdy nevyužili a nemají to ani v plánu. Letos se toto číslo snížilo na pouhých 12 %. [17]

I při tvorbě a provozu mobilních aplikací se nezapomíná na bezpečnost, proto se zabezpečeny přihlašovacími údaji a heslem. Oba tyto bezpečnostní prvky mají mnoho podob, ať už jsou tvořeny čísly nebo písmeny a znaky. Také se začíná integrovat do mobilních aplikací platforma Touch ID, neboli přihlašování pomocí otisku prstu. Tuto možnost zabezpečení nabízí pouze některé banky v České republice. Diskutuje se však o nahrazení hesel a přihlašovacích jmen právě otiskem prstu nebo jako o doplňujícím bezpečnostním prvku, který výše zmíněné nenahrazuje, ale doplňuje. Otisky prstu klienta jsou standardně uloženy v jeho mobilním telefonu, tudíž se do banky neposílají. Pokud kontrola pomocí otisku prstu selže, používá se většinou pro identifikaci již přednastavené heslo, které slouží jako alternativa. Klíčový moment při užívání této platformy nastává v okamžiku, kdy hovoříme o rizicích, která se k užívání pojí. Je použití této platformy opravdu skutečně velkým rizikem nebo naopak snižuje nebezpečí zjištění hesla a přihlašovacího jména do mobilní aplikace? Protože je tato technologie u nás vcelku

čerstvá záležitost nelze jednoznačně říct, že zvyšuje riziko zneužití účtu. Více technologii Touch ID vysvětluje společnost Apple. Dle Apple Inc. (2015) je každý otisk prstu jedinečný, takže je malá šance, že malé části dvou odlišných otisků prstů budou dostatečně shodné pro Touch ID. Pravděpodobnost toho, že se to stane je 1:50 000 pro jeden nasnímaný prst. Je to mnohem lepší než pravděpodobnost 1:10 000, že někde uhodne typický 4 číselný kód pro přístup do Vašeho zařízení. Navíc některé kódy typu ‚1234' mohou být mnohem snadněji uhodnutelné, neexistuje něco jako snadno uhodnutelný vzorek otisku prstu. Naproti tomu pravděpodobnost 1:50 000 značí, že je potřeba více než 50 000 pokusů různých otisků prstů, než náhodně najdete shodu. Funkce Touch ID umožňuje pouze 5 neúspěšných pokusů otisků prstu, poté vyžaduje vložení kódu, bez kterého se do zařízení nedostanete. Pro kompletní konfiguraci Touch ID je nezbytné nastavit číselné heslo. Touch ID je vytvořeno pro snížení používání číselného kódu, ale tento kód bude nastaven jako druhé doplňující bezpečnostní opatření. [18]

Co se týče negativních stránek tohoto způsobu zabezpečení, tak v dnešní době nejsou známy. Použití Touch ID, jako bezpečnostního prvku, je v mobilních aplikacích bank teprve čerstvou záležitostí, tudíž nelze rizika přesně vymezit.
S užíváním mobilní aplikace má velmi blízko technologie NFC. Je to technologie, která umožňuje realizovat platby přímo mobilním telefonem. Pro lepší představu se jedná o kompletní náhradu platební karty. U obchodníka byste tedy při placení nevytahovali z peněženky kartu, ale pouze mobilní telefon, který k terminálu přiložíte. Tato služba je v České republice teprve na vzestupu, v tuto chvíli ji podporuje pouze operační systém Android. Za negativní stránku této technologie je možné považovat samotné zneužití mobilního telefonu, který technologii NFC podporuje. Vzhledem k tomu, že některé banky mohou PIN kód při každé platbě požadovat a některé ne, jedná se v tomto případě pouze o částečné riziko.

Závěrem této podkapitoly je nezbytné doplnit, že v případě ztráty zařízení, ve kterém je mobilní aplikace nahrána je doporučeno tuto situaci okamžitě ohlásit konkrétní bance, která provede příslušná opatření proti zneužití klientova účtu.

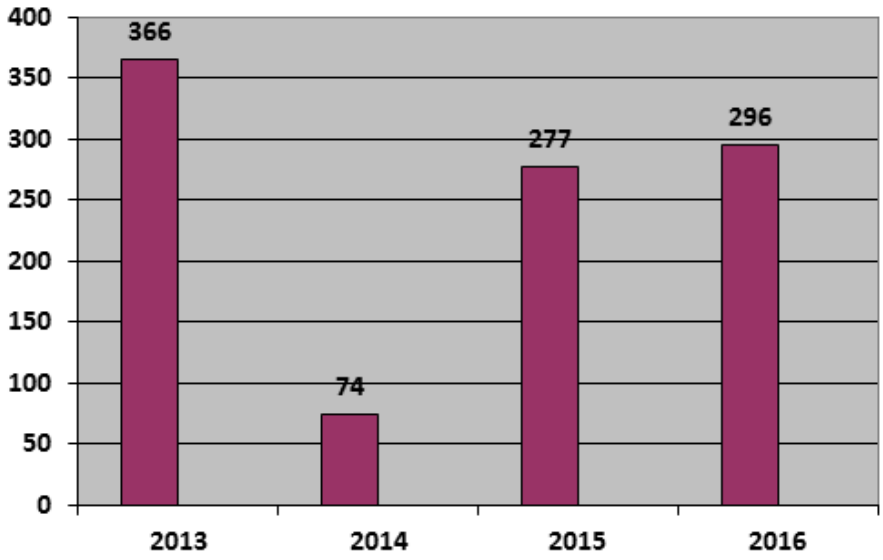
5.2 Rizika nepřímo ovlivnitelná klientem

5.2.1 Rizika spojená s užitím bankomatu

Snaha o cílené napadení účtů klientů bank se řadí mezi každodenní nebezpečí, s kterým se samotné banky potýkají. Mezi ně s řadí například i nasazení skimmovacího zařízení na konkrétní bankomaty různých bank. Skimmovací zařízení je forma hardwaru, který získává informace o platební kartě majitele. Může mít mnoho podob, ale mezi nejčastější patří věrná kopie číselníku nebo třeba mini kamera, která snímá zadávání PIN kódu. Dále je pak doplněn o falešný slot pro platební kartu, reálně kartu tedy nevložíte do slotu na bankomatu, ale pouze do jeho

kopie, která následně okopíruje platební kartu a údaje pošle iniciátorovi celého podvodu. Po získání údajů se iniciátor dostává k financím na účtu majitele platební karty. Statistice skimmingu se věnuje Policie České republiky.

Policie České republiky (2017) uvádí, že národní centrála proti organizovanému zločinu SKPV registrovala v roce 2016 celkem 296 skimmingových útoků, což ve srovnání s rokem 2015 znamená mírný nárůst. Z hlediska lokality bylo v roce 2016 nejvíce skimmingových útoků spácháno na území hlavního města Prahy. K dalším regionům, kde došlo ke skimmingu, patří Liberecký kraj, Středočeský kraj a Jihomoravský kraj. Organizovanou trestnou činností v oblasti padělání platebních karet se i v loňském roce zabývaly skupiny převážně bulharských a rumunských občanů. V roce 2016 nebyl zaregistrován žádný skimmingový útok na tzv. POS terminálech a rovněž nebyl registrován skimming u tzv. bezkontaktních platebních karet. [19]



Obr. 1 Statistika skimmingu.

Zdroj: Policie České republiky, 2017. [19]

Obr. 2 Ukázka nasazení nelegální čtečky do antiskimmovacího nástavce.

Zdroj: Policie České republiky, 2017. [19]

Obr. 3 Lišta, ve které je uložena mikrokamerka a další elektronické součástky – její umístění je obvykle takové, aby mikrokamerka mohla zachytit zadávání PIN kódů – v horní části bankomatu či v horní části nad obrazovkou, popřípadě v místě otvoru pro výdej hotovosti.

Zdroj: Policie České republiky, 2017. [19]

Obr. 4 Ukázka falešné klávesnice

Zdroj: Europol.europa.eu, 2012. [20]

Na použití bezkontaktních karet navážeme v souvislosti s bezkontaktními bankomaty, které se v poslední době začínají objevovat na území České republiky. První bankomat s bezkontaktní čtečkou byl spuštěn v září v roce 2016. Bezkontaktní čtečka zamezuje instalaci skimmovacího zařízení. Tato úroveň byla ještě více posunuta směrem vzhůru spuštěním zcela bezkontaktního bankomatu, s kterým se dá manipulovat pouze skrze dotykovou obrazovku a bezkontaktní čtečku. Bankomat tohoto typu je první na světě a hovoří se o možnosti vybírat i za pomocí mobilního telefonu s technologií NFC, a také o instalaci dalších bankomatů stejného typu. Tento způsob vybírání by zamezil například instalaci skimmovacího zařízení v podobě falešné klávesnice, kterou v tomto případě plně nahrazuje dotyková obrazovka. Více o bankomatu se dozvíme na stránkách Air Bank a.s. (2017), která doplňuje, že testovaný bankomat nemá ani klasickou klávesnici pro zadání PINu. PIN se místo toho zadává přímo na zašifrovaném dotykovém displeji. Spolu s bezkontaktní čtečkou tak nový bankomat omezuje riziko zadržení karty a okopírování PINu někým nepovolaným. Testovaný bankomat je také přibližně dvakrát rychlejší než současné modely a celý výběr zvládne zpracovat do 14 vteřin. Počítá také s tím, že lidé sledují změny zůstatků přes mobilní aplikaci nebo SMS zprávy, a nemá tiskárnu pro tisk stvrzenek. [21]

Obr. 5 Ukázka bezkontaktní čtečky

Zdroj: Aktuálně.cz, 2016. [22]

Obr. 6 První bezkontaktní bankomat na světě

Zdroj: Air Bank a.s., 2017. [21]

Obr. 7 Srovnání standardního a bezkontaktního bankomatu

Zdroj: Air Bank a.s., 2017. [21]

Obr. 8 Srovnání standardního a bezkontaktního bankomatu

Zdroj: Air Bank a.s., 2017. [21]

Jak se proti tomu bránit?

Při použití konkrétního bankomatu si všímat detailů, pokud se bude držiteli platební karty zdát něco podezřelé, je lepší bankomat nevyužívat. Dále používat pro výběry frekventovaná místa, kde je výskyt skimmovacích zařízení nižší nebo používat pro výběry výše zmíněné bankomaty s bezkontaktní čtečkou či zcela bezkontaktní bankomat.

5.2.2 Rizika vytvořená uměle

V této kapitole se budeme věnovat rizikům, která jsou nebo byla v minulosti vytvořena uměle. Lze si pod tím představit situace, které jsou vytvořeny třetí osobou za účelem vyvolání paniky nebo paranoi mezi klienty českých, ale i zahraničních bank.

V posledních letech se mezi tato rizika může řadit například zadání PIN kódu obráceně. Umělost spočívá v mylné informaci, která tvrdí, že zadáním tímto způsobem je přivolána k bankomatu Policie, která by v případě nebezpečí zneužití účtu okamžitě zasáhla. Když hovoříme o zneužití účtu, v této situaci se jedná o přepadení třetí osobou majitele platební karty, který se právě snaží z bankomatu vybrat hotovost.

Dalším případem je kauza platebních terminálů v kapse. Narážíme tím na situaci, kdy má daný útočník v kapse, nebo jiném místě, uložen platební terminál, který přijímá automaticky bezkontaktní platby do výše 500 korun. Útočníkovi stačí pouze přijít do blízkého okolí nic netušícího člověka terminál přiložit na místo, kde má pravděpodobně uchovanou kartu a peníze z ní nepozorovaně odečíst. Nelze říci, že je to vyloženě technicky neproveditelné, nicméně není možné tento podvod zrealizovat anonymně. Tudíž je tento čin trestně postižitelný a celkem lehko dohledatelný, lze jej řadit mezi uměle vytvořená rizika.

Někteří klienti bank mohou žít v představě, že lze zneužít jejich bankovní účet za pomocí čísla účtu, variabilních symbolů nebo symbolů, které se využívají hlavně při zahraničních platbách – IBAN, SWIFT, BIC, ABA kód a další. Poskytnutím těchto dat není možné bankovní účet zneužít, pokud si však klient není při transakci jistý, zda údaje, které po něm kupující chce nehraničí s bezpečím jeho účtu, není ostudné a ani pošetilé konkrétní případ konzultovat s pracovníkem banky, který by měl být v této situaci nápomocen.

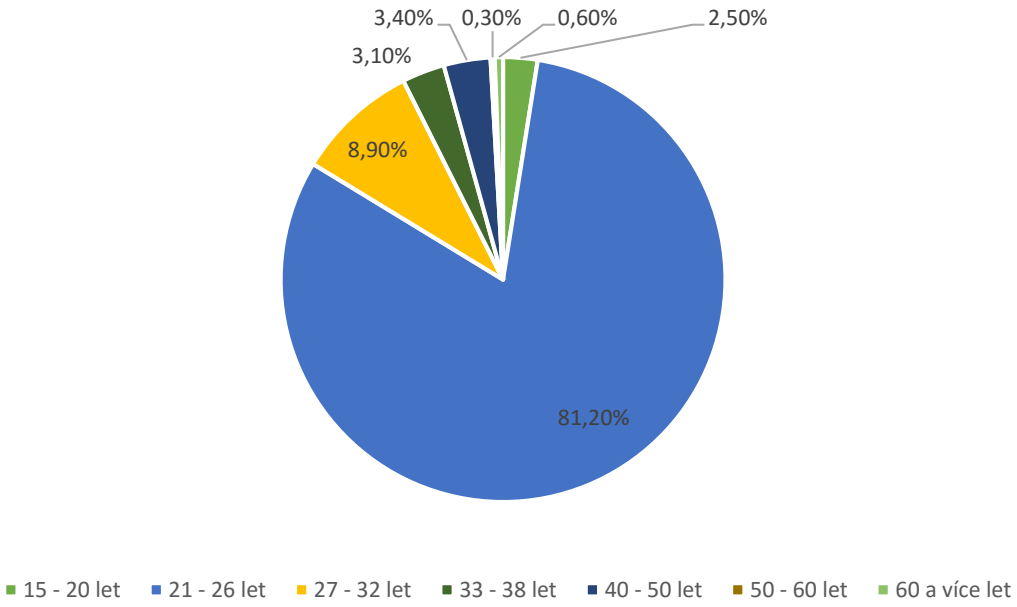
Uměle vytvořených rizik může být celá řada a neustále přibývají, je možné snižovat riziko jejich výskytu vyvracováním různých virálních kauz, které se šíří buďto prostřednictvím sociálních sítí nebo jinak.

5.3 Chování klientů bank ve vztahu k bankovnímu účtu

Před kategorizací výše uvedených rizik byl za pomocí sociálních sítí rozeslán dotazník pro zjištění úrovně povědomí o rizicích, která se pojí s vedením bankovního účtu. Celkový počet respondentů, kteří se dotazníku zúčastnili a odpověděli na všechny otázky, bylo 325. Respondenti byli náhodně vybráni z různých věkových kategorií. V dotazníku bylo celkem 19 otázek, kde byla pouze možnost jedné odpovědi. Protože byla pro rozeslání použita hlavně sociální síť, byla návratnost 100 %. Předpokladem pro vyplnění dotazníku byl fakt, že respondent vlastní bankovní účet, který aktivně používá.

Vyhodnocení

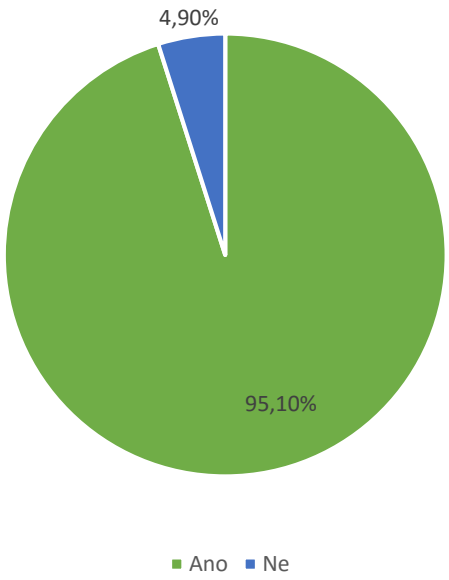
První otázka v dotazníku se zaměřovala na věkovou kategorii, v niž se respondenti nacházejí. Největší počet respondentů byl ve věkové kategorii mezi 21 až 26 lety, celkem se tedy jednalo o 81,20 %.



Obr. 9 V jaké jste věkové kategorii?

Zdroj: Vlastní zpracování, 2017.

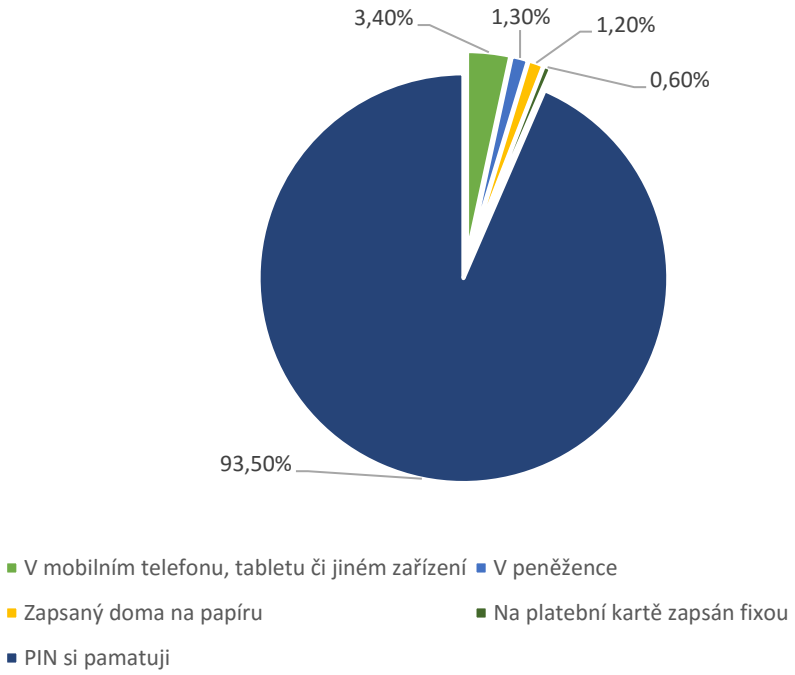
Další část dotazníku se týkala možných rizik, které se s vlastnictvím účtu mohou pojit. Byl cílen na konkrétní případy, které mohou zvyšovat riziko zneužití bankovního účtu. Na toto téma úzce navazuje otázka, zda si respondent pamatuje svůj PIN kód nebo ho má někde poznačený.



Obr. 10 Pamatujete si svůj PIN kód k platební kartě?

Zdroj: Vlastní zpracování, 2017.

V tomto případě došlo k překvapivému zjištění, 95,10 % respondentů si PIN kód k platební kartě pamatuje. K tomuto výsledku může vést skutečnost, že většina bank v České republice umožňuje nastavení vlastního, tedy pro některé jedince nejspíše lépe zapamatovatelného, PIN kódu. Otázkou zůstává, zda formát PIN kódu není příliš snadno předvídatelný, konkrétněji v jakém je tvaru? Zda je jeho součástí datum či rok narození? Tato otázka nemohla být v dotazníku položena z důvodu bezpečnosti. Nicméně bylo možné zjistit, jakým způsobem si lidé uchovávají svůj PIN kód, pokud si jej nepamatují.

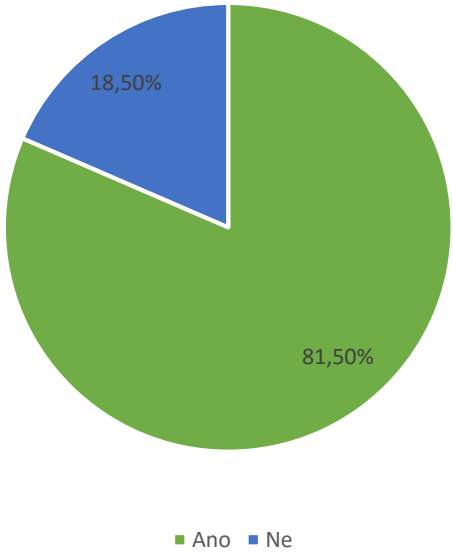


Obr. 11 Pokud si PIN kód nepamatujete, kde ho máte uchován?

Zdroj: Vlastní zpracování, 2017.

Celkový počet respondentů, kteří si PIN kód uchovávají jinde, než ve své mysli je 6,50 %. Jakýkoli zápis PIN kódu lze považovat za nebezpečný a zvyšující riziko zneužití bankovního účtu konkrétního respondenta. Doporučuje se ponechávat si PIN kód zvolený bankou nebo si zvolit svůj vlastní. Důležité však je si PIN kód nikde nezapisovat a nikomu dalšímu ho nesdělovat, a to ani v případě nouze.

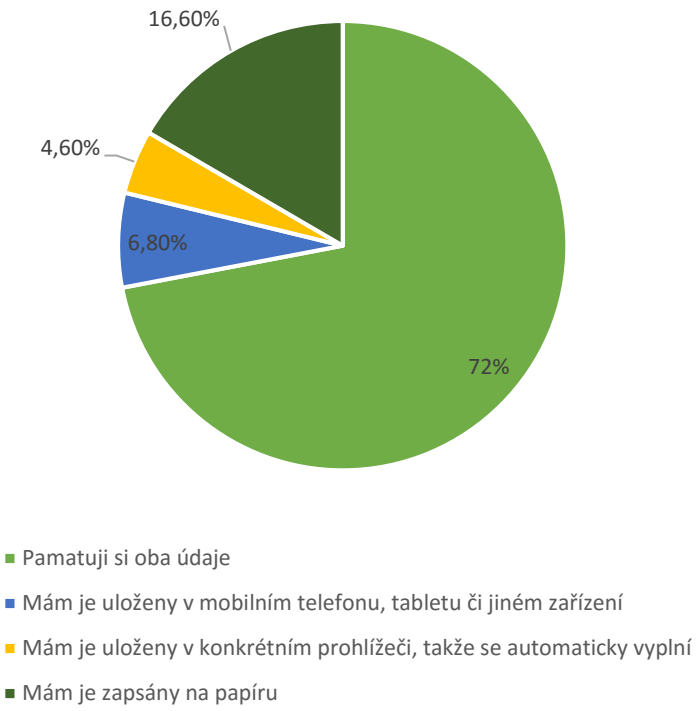
Poté navážeme na téma, které je se zapamatováním PIN kódu úzce spojeno. Hovoříme o přihlašovacím údaji a hesle do internetového bankovnictví klientů bank.



Obr. 12 Pamatujete si své přihlašovací údaje, včetně hesla, do internetového bankovnictví?

Zdroj: Vlastní zpracování, 2017.

U této otázky bylo zjištěna celkem překvapivá skutečnost, 18,50 % respondentů si nepamatuje své přihlašovací údaje a heslo do internetového bankovnictví. Příčinou může být to, že banky tyto údaje klientům generují, klient si ne vždy, volí sám. Pokud si je klient nepamatuje, někam si je zaznamená, což není pozitivní zjištění. Kam si klient banky údaje nejčastěji zapisuje je zobrazeno na následujícím obrázku.



Obr. 13 Jakým způsobem uchováváte přihlašovací údaje a heslo pro přihlášení do internetového bankovnictví?

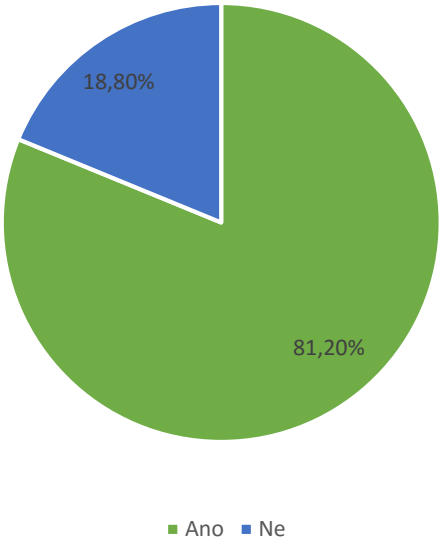
Zdroj: Vlastní zpracování, 2017.

Největší podíl respondentů si údaje pamatuje, jedná se tady o 72 %. Nejčastěji si respondenti zapisují údaje na papír, a to v 16,60 % případů. Také pro zápis používají mobilní telefony, tablety či jiná zařízení anebo je mají uloženy v konkrétním internetovém prohlížeči. Pod tuto možnost spadá i instalace doplňků webových prohlížečů, které hesla dokáží uchovávat. Ani jeden z výše zvolených způsobů uchovávání údajů není žádoucí z důvodu zneužitelnosti. Pokud by byl notebook odcizen nebo ztracen či s ním bylo nakládáno neoprávněnou osobou, mohlo by dojít ke zneužití daného účtu, což není žádoucí. Proto se doporučuje si údaje opět pamatovat, nikde je nezapisovat a s nikým nesdílet. V neposlední řadě se doporučuje údaje jednou za čas obměnit. Více se tématu věnoval Týden.cz (2016), který uvedl, že klienti bank se o bezpečnost v on-line prostředí stále příliš nezajímají. Index bezpečnosti České bankovní asociace, který sleduje vybraná kritéria bezpečného působení na internetu, se za poslední tři roky téměř nezměnil. V růstu mu brání především nechuť měnit hesla a PIN kódy.
[23]

Když by daný majitel účtu chtěl nějakým způsobem poskytnout bezpečnou cestou přístup ke svému účtu, nabízí se možnost založení takzvaného disponenta, který může s účtem pracovat. Banky v České republice rovněž nabízejí vydání karty

pro dalšího uživatele, který není přímo majitelem daného účtu, této funkci se zpravidla říká držitel. Je nezbytné se o obou možnostech poskytnutí práv jiné osobě informovat přímo ve své bance.

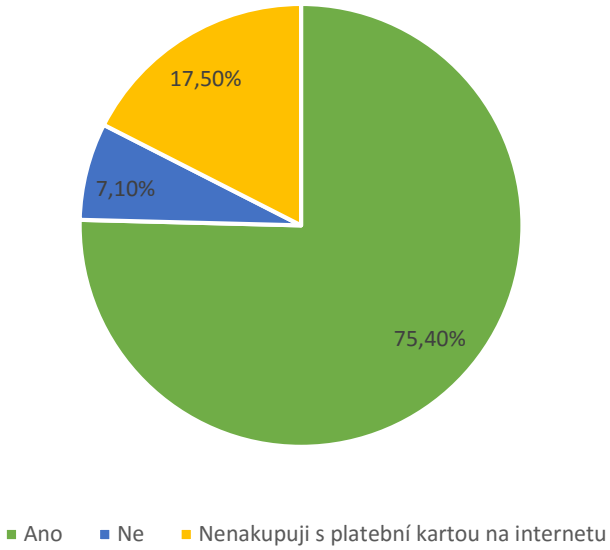
Další otázky byly cíleny na platební karty a jejich používání respondenty. Stěžejní otázkou bylo, zda respondenti platí s platební kartou na internetu a na to navazující otázky. Cílem těchto otázek bylo zjistit, zda jsou si nakupující vědomi, že každá webová stránka může mít jiné obchodní podmínky, a ne vždy obsahují podmínky, s kterými, v době nákupu, respondent souhlasí. Nedorozumění vzniká hlavně z důvodu nízké ostražitosti a následnému odsouhlasení například pravidelnému strhávání plateb v určité výši.



Obr. 14 Platíte s platební kartou na internetu?

Zdroj: Vlastní zpracování, 2017.

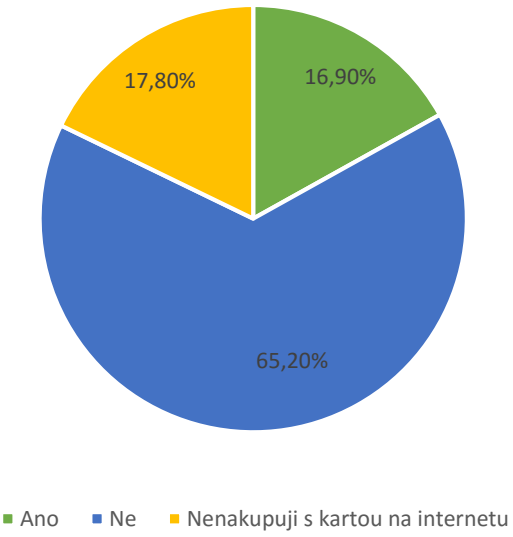
Většina respondentů s platební kartou na internetu platí a z výsledků, které vyplynuly z následující otázky, je zřejmé, že si pro nákupy vybírají internetové stránky, které určitým způsobem znají. Mohou je znát z televizních reklam, od známých nebo například z recenzí na internetu.



Obr. 15 Nakupujete se svojí kartou na stránkách, které znáte?

Zdroj: Vlastní zpracování, 2017.

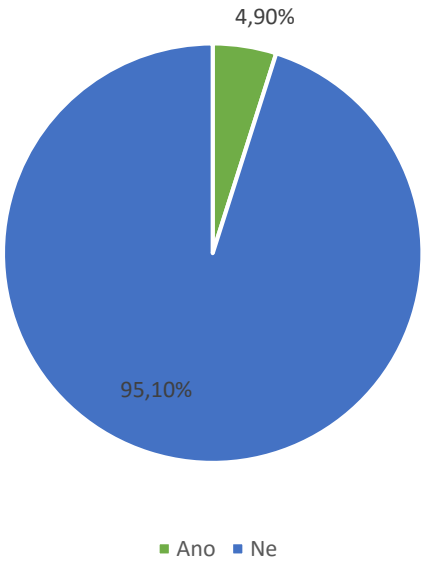
I přesto, že 81,20 % respondentů nakupuje s platební kartou na internetu a 75,40 % na stránkách, které jsou pro ně známé, drtivá většina si nečte obchodní podmínky daných stránek. Mluvíme o 65,20 % respondentů, kteří aktivně nakupují platební kartou na internetu a nečtou obchodní podmínky. Při nákupu na stránkách, které nejsou důvěryhodné nebo mohou být podvodné je tento počet více než alarmující a je nezbytné informovat majitele platebních karet o rizicích, která jsou s tímto spojená.



Obr. 16 Čtete si obchodní podmínky před zadáváním čísla své platební karty na stránce, kde se chystáte něco koupit?

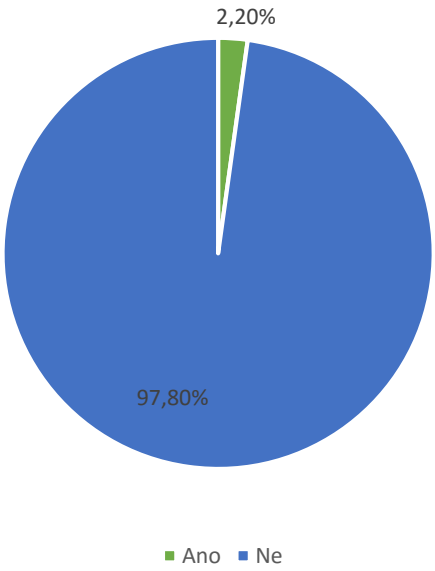
Zdroj: Vlastní zpracování, 2017.

Co se týče zkušeností respondentů se zneužitím jejich platební karty, tak jsou nízké. Tento jev je žádoucí, pouze 4,90 % má se zneužitím karty zkušenost. Z toho u 2,20 % došlo ke zneužití karty vlastní nepozorností nebo vinou. Důvod, proč se tak stalo, nebyl dále rozveden z důvodu bezpečnosti.



Obr. 17 Byla Vaše platební karta v minulosti zneužita?

Zdroj: Vlastní zpracování, 2017.

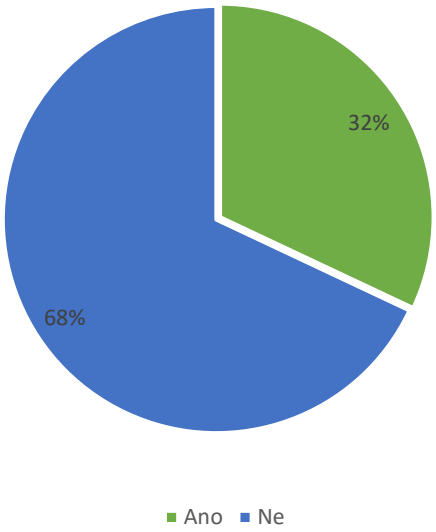


Obr. 18 Byla karta zneužita Vaší nepozorností / vinou?

Zdroj: Vlastní zpracování, 2017.

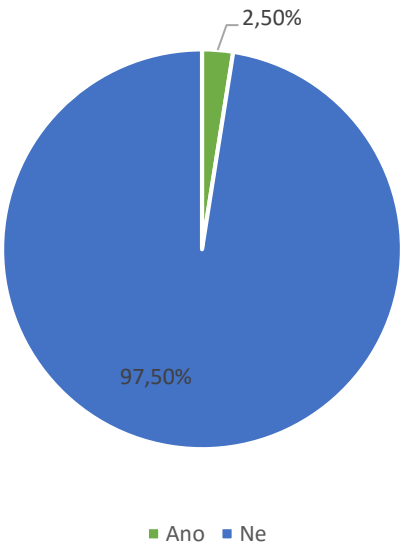
Platební kartu zapůjčilo osobě, kterou zná 32 % - tedy 104 z 325 respondentů. Po zapůjčení byla karta zneužita 2,50 % respondentům. Zapůjčení platební karty cizí osobě se považuje za porušení obchodních podmínek a může vést k jejímu zneužití. Důsledky tohoto zapůjčení mohou být tragické. Majitel karty nemá přehled o

operacích, které s ní daná osoba provádí. V případě, kdy chce majitel účtu svěřit své finance jiné osobě, lze to vyřešit i jinou cestou, která byla popsána výše. Jedná se o nastavení práva u funkce, která se může nazývat držitel.



Obr. 19 Půjčil(a) jste někdy svoji platební kartu jiné osobě, kterou znáte?

Zdroj: Vlastní zpracování, 2017.

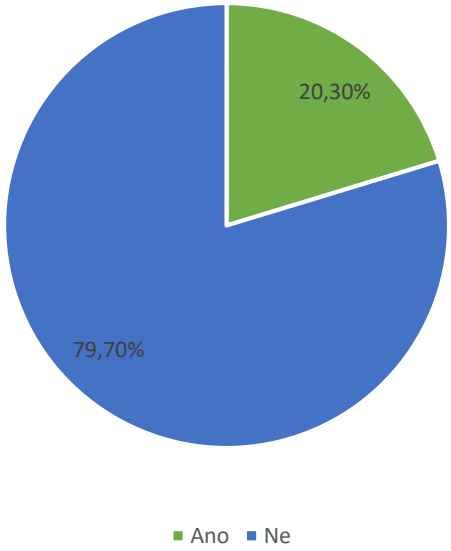


Obr. 20 Byla Vaše karta později (po zapůjčení) zneužita?

Zdroj: Vlastní zpracování, 2017.

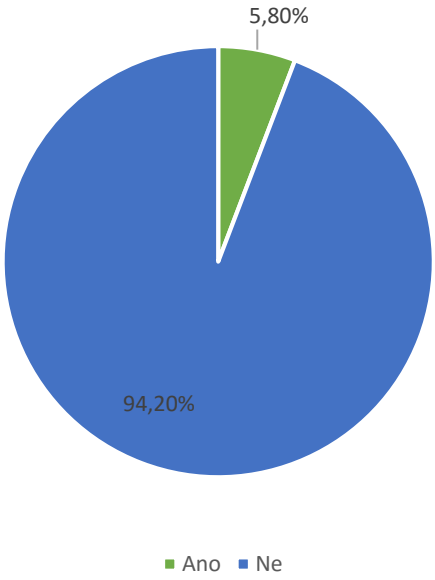
Často diskutovaným tématem je zneužití účtů na základě cílených útoků, které můžeme vyhledat pod názvem „phishing“. Tohle diskutované téma nemohlo chybět

v dotazníku, tudíž do něj bylo zařazeno a přineslo zajímavé výsledky. S phishingem se setkalo 20,30 % respondentů a 5,80 % se řídilo pokyny, které nalezli v SMS zprávě nebo e-mailu. Účet byl zneužit pouze 1,80 %, což značí vysokou úroveň efektivity bank v boji proti cíleným útokům na účty svých klientů.



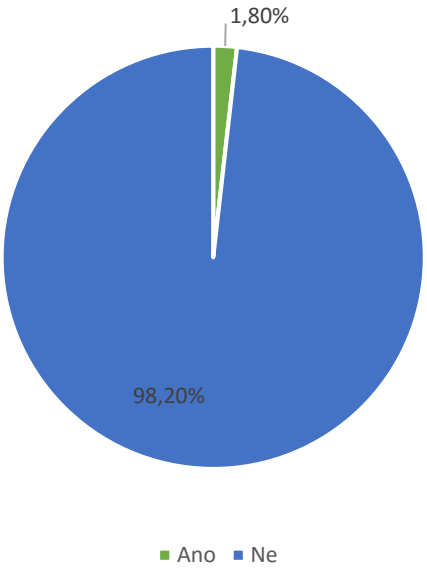
Obr. 21 Setkal(a) jste se někdy s cíleným útokem na Váš účet, který proběhl formou SMS zprávy nebo e-mailem za účelem získat Vaše přihlašovací údaje?

Zdroj: Vlastní zpracování, 2017.



Obr. 22 Použil jste odkaz, který se v e-mailu/SMS zprávě nacházel a postupoval podle pokynů?

Zdroj: Vlastní zpracování, 2017.



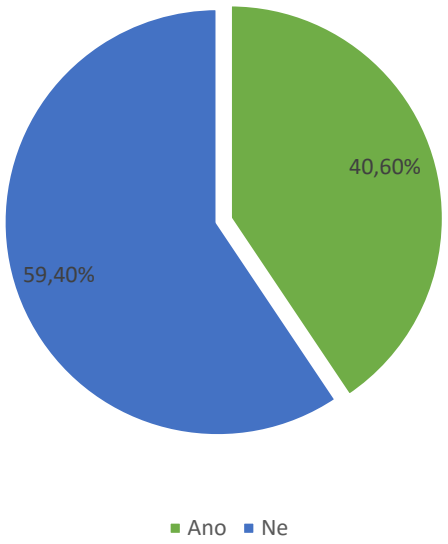
Obr. 23 Byl Váš účet na základě této útočné SMS zprávy/e-mailu následně zneužit?

Zdroj: Vlastní zpracování, 2017.

Proti phishingu se neustále bojuje a banky se snaží jej dostat do povědomí svých klientů. Protože se ale vynalézavost útočníků stále zdokonaluje, je nezbytné zapracovat na neustálém zvyšování informovanosti klientů bank všemi možnými prostředky a poučit je, jak se zachovat v případě, že dostanou podezřelý e-mail nebo SMS zprávu. Jeden z rozsáhlejších úroků popsal i server iDnes.cz (2017), který ve své elektronické publikaci zmínil, že mezi uživateli mobilních telefonů s operačním

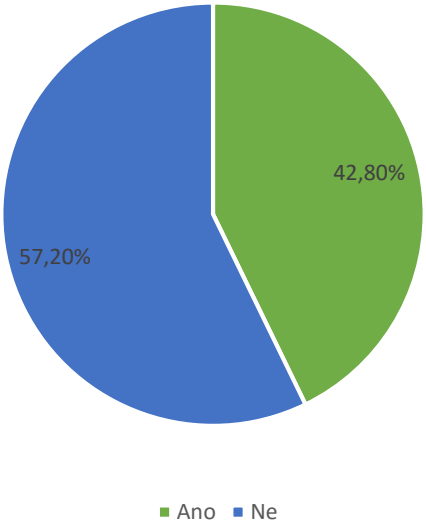
systémem Android se množí podvodné SMS vyzývající jménem České pošty ke stažení aplikace „Pošta Online“. Odkazují na internetové stránky se škodlivým programem. Trojský kůň, kterého si uživatel nevědomky do mobilu stáhne, útočí na elektronické bankovnictví uživatelů. Pošta podle mluvčího pošty Matyáše Vitíka zatím zaznamenala asi desítku případů. I když není zatím jasné, zda vir dokáže zachytit i ověřovací SMS internetového bankovnictví, je i tak nebezpečný. V minulých letech se jménem České pošty šířily podvodné e-maily, které se vydávaly za zprávy o sledování poštovní zásilky. Podvodné e-maily obsahovaly odkaz vedoucí na web, který do počítače stáhl škodlivý kód. Útočníci však většinou přímo útočí na uživatele konkrétního internetového bankovnictví prostřednictvím e-mailů nebo sociálních sítí. [24]

Poslední sada otázek se soustřeďuje na to, zda klienti bank používají jejich mobilní aplikace, a také jaké mají v této oblasti znalosti. Mobilní aplikaci používá 40,60 % respondentů a 42,80 % ví, co se skrývá pod pojmem Touch ID. Touch ID je celkem diskutované téma ve spojení s mobilními aplikacemi bank. Existují různé pohledy na to, jak tuhle formu zabezpečení chápat. Nelze ani na jeden z názorů nahlížet ryze pozitivně nebo zcela negativně. Přihlašování pomocí Touch ID je v tuhle chvíli na vzestupu nelze hovořit o rizicích, která jsou s ní přímo spojená.



Obr. 24 Používáte mobilní aplikaci své banky?

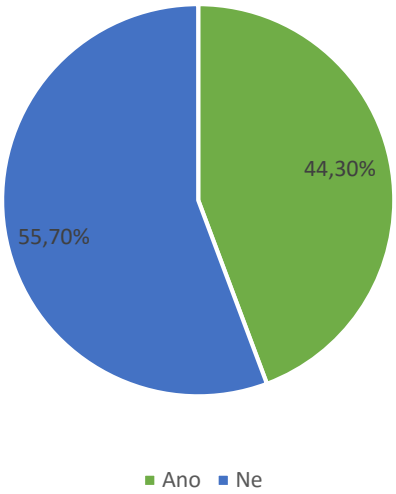
Zdroj: Vlastní zpracování, 2017.



Obr. 25 Víte, co je to Touch ID?

Zdroj: Vlastní zpracování, 2017.

Dalším otevřeným tématem je v České republice technologie NFC, pod kterou si něco dokáže představit 44,30 % respondentů. Opět se jedná o technologii, která není v naší zemi příliš známá a lze o ní říci, že se posouvá kupředu.



Obr. 26 Víte, co si představit pod pojmem NFC?

Zdroj: Vlastní zpracování, 2017.

Na závěr je nezbytné k vyhodnocení dodat, že pokud si klient banky není jistý, zda nebyla porušena bezpečnost jeho účtu na základě jeho chování, je doporučeno neprodleně kontaktovat banku a celou situaci oznámit a patřičně popsat.

Protože míru finanční gramotnosti je nezbytné z důvodu neustálého pokroku navyšovat, je žádoucí, aby i bankovní instituce byly do této problematiky více zapojeny. Některé banky se už v tuto chvíli snaží být více otevřenější a pro ‚normálního' občana vytvářejí přátelštější a lidštější přístup. Pokud se zapojí i do zvyšování povědomí o rizicích, která jsou s vedením bankovního účtu spojená nebo i třeba o umělých rizicích, prostřednictvím sociálních sítí, které jsou v dnešní době velice využívány, je reálné zvýšit míru finanční gramotnosti obyvatel a chránit tak jejich účty i nepřímou formou.

Pro kompletnost je doplněna důležitá poznámka. V systémovém pojetí se vždy u příčinných problémů pracuje se systémem podstatných veličin. Protože je z tohoto pohledu tato diplomová práce atypická – kategorizují se v ní rizika, je i přesto možné z toho, co tato rizika ovlivňuje vytipovat důležité podstatné entity, které je ovlivňují. Hovoříme zejména o entitách – člověk, okolí a aktivace. Důležitost těchto entit je již dána dle pořadí, v kterém byly zapsány.

S oborovými vlastnostmi entity, tedy vlastnost člověka – jeho mysl, se můžeme setkat např. u obrázků číslo 10, 11, 12, 13 a dalších. Okolí entity můžeme pozorovat například na obrázcích číslo 15, 17, 20 a 23. Aktivace je zcela jasně demonstrována na obrázku číslo 14.

6 Závěr

Podstatou diplomové práce bylo změnit nestandardní problémovou situaci na standardní. Na tuto práci bylo nahlíženo systémově. Systémové pojetí rizik v této práci, spočívá i ve faktu, že byla řešena znalostním modelováním, kde modelovým objektem byly znalosti subjektu – jedné osoby.

První část práce je zaměřena na literární rešerši a vysvětlení pojmů vztahujících se k řešenému tématu. V druhé části byl vytvořen soubor rizik a jejich následná kategorizace, která byla vytvořena na základě získané praxe a zkušeností v daném oboru. Pro získání informací o povědomí klientů bank ve vztahu k vedením bankovního účtu byl vypracován dotazník, který byl následně za pomocí sociálních sítí rozeslán mezi respondenty. Dotazník se skládal z 19 otázek, které byly zaměřeny na chování klientů bank ve vztahu k jejich bankovnímu účtu. Celkem se dotazníku zúčastnilo 325 respondentů a data z něj byla posléze statisticky zpracována a vykreslena za pomocí grafů v programu MS Excel.

Z výše uvedeného dotazníku byl rozlišen systém důležitých entit, které rizika ovlivňují – člověk, okolí a aktivace. Většina kategorizovaných rizik, která se v práci vyskytují, jsou spojena s člověkem, a proto je důležité tuto problematiku rozpracovat a dát ji do povědomí lidí.

Závěrem lze říci, že pokud lidé chtějí snížit rizika, musí začít pracovat na sobě. Konkrétní rizika v této diplomové práci se dají snižovat zvyšováním finanční gramotnosti člověka.

7 Seznam použitých zdrojů

[1] Ministerstvo financí České republiky. *Měření finanční gramotnosti 2015: Kompletní výsledky*. [online] 2016. [cit. 25-04-2017] Dostupné z: http://www.psfv.cz/cs/pro-odborniky/mereni-urovne-financni-gramotnosti/2015/mereni-urovne-financni-gramotnosti-2784

[2] Česká bankovní asociace.cz. *Banky a fakta: Hotovost, nebo platba kartou?* [online] 2016. [cit. 25-04-2017] Dostupné z: https://www.czech-ba.cz/sites/default/files/baf_hotovost_vs_karta.pdf

[3] Marvanová, M., Houda, M. a kol. *Platební styk: platební a zajišťovací instrumenty ve vnitřním a zahraničním obchodě*. Brno: ECON, 1995. ISBN 80-901627-2-X

[4] Máče, M. *Platební styk klasický a elektronický*. Praha: Grada, 2006. ISBN 80-247-1725-5

[5] Česká bankovní asociace.cz, *Spotřebitelský slovníček*. [online] 2017. [cit. 26-04-2017] Dostupné z: https://www.czech-ba.cz/cs/bankovni-sektor/bankovni-pojmy/spotrebitelsky-slovnicek

[6] Viswanathan, P. - Lifewire.com. *What is a Mobile Application?* [online] 2016. [cit. 26-04-2017] Dostupné z: https://www.lifewire.com/what-is-a-mobile-application-2373354

[7] Chell, D., Erasmus, T., Colley, S., Whitehouse, O. *The Mobile Application Hacker's Handbook*. Indiana: John Wiley & Sons Ltd., 2015. ISBN 978-1-118-95850-6

[8] Coskun, V., Ok, K., Ozdenizci, B. *Near Field Communication: from theory to practice*. United Kingdom: John Wiley & Sons Ltd., 2012. ISBN 978-1-119-97109-2

[9] Janíček, P., Marek, J. *Expertní inženýrství v systémovém pojetí*. Praha: Grada, 2013. Expert (Grada). ISBN 978-80-247-4127-7

[10] Tichý, M. *Ovládání rizika: analýza a management*. Beckova edice ekonomie. Praha: C.H. Beck, 2006. ISBN 80-7179-415-5

[11] Rais K., Smejkal V. *Řízení rizik ve firmách a organizacích*. Praha: Grada, 2013. ISBN 978-80-247-4644-9

[12] Fotr J., Hnilica J. *Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování*. Praha: Grada, 2009. ISBN 978-80-247-2560-4

[13] Fotr J., Hnilica J. *Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování*. 2. aktualiz. a rozš. vyd. Praha: Grada, 2014. Expert (Grada). ISBN 978-80-247-5104-7.

[14] FOTR, J. *Tvorba strategie a strategické plánování: teorie a praxe*. Praha: Grada, 2012. Expert (Grada). ISBN 978-80-247-3985-4.

[15] Independent.co.uk, *Constantly checking your mobile phone can lead to ‚cognitive failures'*. [online] 2015. [cit. 26-04-2017] Dostupné z: http://www.independent.co.uk/life-style/gadgets-and-tech/news/constantly-checking-your-mobile-phone-can-lead-to-cognitive-failures-10458210.html

[16] Český statistický úřad. *Informační společnost v číslech 2016*. [online]. 2016. [cit. 26-4-2017]. Dostupné z: https://www.czso.cz/csu/czso/informacni-spolecnost-v-cislech-2016

[17] VISA.cz, *Mobilní platby rostou rapidní rychlostí, ukazuje průzkum společnosti Visa*. [online]. 2016. [cit. 26-4-2017]. Dostupné z: https://www.visa.cz/o-nas/tisk-media/mobilni-platby-rostou-rapidni-rychlosti-ukazuje-pruzkum-spolecnosti-visa-1609019?returnUrl=/o-nas/tisk-media/listing

[18] Apple Inc., *About Touch ID security on iPhone and iPad*. [online]. 2015. [cit. 26-4-2017]. Dostupné z: https://support.apple.com/en-us/HT204587

[19] Policie České republiky. *Skimming*. [online]. 2017. [cit. 26-4-2017]. Dostupné z: [http://www.policie.cz/clanek/skimming-2011.aspx]

[20] Europol.europa.eu, *Payment Card Fraud in the European Union – Europol*. [online]. 2012. [cit. 26-4-2017]. Dostupné z: https://www.europol.europa.eu/sites/default/files/images/card_skimming_02.preview.jpg

[21] Airbank a.s., *Air Bank v Praze testuje první čistě bezkontaktní bankomat na světě*. [online]. 2017. [cit. 26-4-2017]. Dostupné z: https://www.airbank.cz/novinky/air-bank-v-praze-testuje-prvni-ciste-bezkontaktni-bankomat-na-svete

[22] Aktuálně.cz, *Z bankomatu vyberete bezkontaktně. Novinku spouští první banka v Česku*. [online]. 2016. [cit. 26-4-2017]. Dostupné z: https://zpravy.aktualne.cz/finance/z-bankomatu-vyberete-bezkontaktne-novinku-spousti-prvni-bank/r~1bf3b6c074db11e6a4100025900fea04/?redirected=1495192945

[23] Týden.cz, *Klientům bank je on-line bezpečnost lhostejná*. [online]. 2016. [cit. 26-4-2017]. Dostupné z: http://www.tyden.cz/rubriky/byznys/cesko/klientum-bank-je-on-line-bezpecnost-lhostejna_398517.html

[24] iDnes.cz, *Podvodné SMS útočí na Česko. Tváří se, že jsou z České pošty*. [online]. 2016. [cit. 26-4-2017]. Dostupné z: http://mobil.idnes.cz/android-

vir-ceska-posta-0vl-/mob_tech.aspx?c=A170126_101517_tec-kratke-zpravy_vse

[25] Česká národní banka.cz, *Upozornění České národní banky na rizika spojená s využíváním elektronického bankovnictví*. [online]. 2017. [cit. 22–5-2017]. Dostupné z: https://www.cnb.cz/cs/dohled_financni_trh/vykon_dohledu/upozorneni_pro_verejnost/upozorneni_el_bankovnictvi.html

[26] Komínek, T., Rousek, J. *Rizika elektronického bankovnictví*. [online]. 2007. [cit. 22-5-2017]. Dostupné z: https://is.muni.cz/el/1456/podzim2007/PFKMEB/4168069/Rizika_elektronickeho_bankovnictvi.pdf

8 Seznam obrázků

9 Seznam tabulek

10 Seznam použitých zkratek

GSM – Global System for Mobile communications
SIM – Subscriber Information Module
NFC – Near Field Communication
PIN – Personal Identification Number