Mendelova univerzita v Brně
Provozně ekonomická fakulta

Kybernetické riziko bezhotovostního a elektronického platebního styku

Bakalářská práce

Vedoucí práce:

Ing. Jiří Balej

Kateřina Kuchtová

Brno 2017

Na tomto místě bych ráda poděkovala svému vedoucímu bakalářské práce Ing. Jiřímu Balejovi za vstřícný přístup, cenné rady a věcné připomínky, které mi napomohly k vypracování této práce.

Čestné prohlášení

Prohlašuji, že jsem tuto práci: **Kybernetické riziko bezhotovostního a elektronického platebního styku**
vypracovala samostatně a veškeré použité prameny a informace jsou uvedeny v seznamu použité literatury. Souhlasím, aby moje práce byla zveřejněna v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů, a v souladu s platnou *Směrnicí o zveřejňování vysokoškolských závěrečných prací.*

Jsem si vědoma, že se na moji práci vztahuje zákon č. 121/2000 Sb., autorský zákon, a že Mendelova univerzita v Brně má právo na uzavření licenční smlouvy a užití této práce jako školního díla podle § 60 odst. 1 Autorského zákona.

Dále se zavazuji, že před sepsáním licenční smlouvy o využití díla jinou osobou (subjektem) si vyžádám písemné stanovisko univerzity o tom, že předmětná licenční smlouva není v rozporu s oprávněnými zájmy univerzity, a zavazuji se uhradit případný příspěvek na úhradu nákladů spojených se vznikem díla, a to až do jejich skutečné výše.

V Brně dne 17. května 2017 _____

Abstract

Kuchtová, K. Cyber risk of non-cash and electronic payment. Bachelor thesis. Brno: Mendel University, 2017.
The bachelor thesis is focused on cyber risk of non-cash and electronic payment. The first part of this thesis specifies the most popular electronic payments system and with that linked cyber risks. By questionnaire survey is then determined the extent and frequency of use of non-cash and electronic payment instruments. The survey also investigates the knowledge of users within the cyber security topic as well as the use of security measures and elements of individual instruments. At the same time, thesis should recommend steps to reduce the cyber risk.

Keywords

Cyber risk, cybersecurity, cybercrime, online payment system, payment security

Abstrakt

Kuchtová, K. Kybernetické riziko bezhotovostního a elektronického platebního styku. Bakalářská práce. Brno: Mendelova univerzita v Brně, 2017.
Bakalářská práce se zabývá problematikou kybernetického rizika bezhotovostního a elektronického platebního styku. V literární rešerši jsou popsány nejpoužívanější elektronické platební prostředky a kybernetická rizika spojená s jejich užíváním. Pomocí dotazníkového šetření je zjištěna míra využívání nástrojů bezhotovostního a elektronického platebního styku včetně frekvence placení, ověřeno využívání bezpečnostních opatření a prvků jednotlivých nástrojů a otestována znalost respondentů oblasti kybernetické bezpečnosti. V závěru jsou uvedeny doporučení pro zlepšení informovanosti uživatelů o kybernetických rizicích. Práce by zároveň měla čtenáři doporučit kroky ke snížení kybernetického rizika.

Klíčová slova

Kybernetické riziko, kybernetická bezpečnost, internetová kriminalita, platební styk, zabezpečení platebního styku

Obsah

1 Úvod

Život bez informačních a komunikačních technologií je pro nás již nepředstavitelný. Stává se nedílnou součástí našich životů, a byť jejich sebemenší výpadek může mít až katastrofické následky. Moderní doba internetového připojení patří ke globalizačním faktorům, které umožňují rychlejší tok informací, větší zabezpečení a hlavně zjednodušení práce. Právě díky internetu si můžeme nakoupit zboží či zaplatit za služby z pohodlí našeho domova nebo na cestách. Bohužel, rozvíjení těchto technologií s sebou nese i své stinné stránky. Jednou z nich je počítačová kriminalita.

Ve finančním sektoru koluje nepřeberné množství finančních prostředků a pravděpodobnost útoku hackerů či viru je zde velice vysoká. I přestože má každý platební prostředek několikanásobné zabezpečení, musíme myslet i na rizika používání, kterým je třeba předcházet. Pro zajištění bezpečnosti elektronických plateb je potřeba ověřit identitu uživatele, neboli provést tzv. autentizaci uživatele, při níž si odpovídáme na otázku: „*Je osoba tou, za kterou se vydává*?“, a přiřadit jí oprávnění pro práci v systému tzv. autorizaci.

Z pohledu běžného si uživatele si můžeme všimnout, že jsme již standardně vyzýváni k tvorbě složitějších hesel či prokazování se pomocí SMS kódu. A vzhledem k tomu, že internet pracuje s našimi penězi, je jeho bezpečnost prvořadou záležitostí. Systém ochrany se skládá z několika základních a na sobě nezávislých prvků, a jakmile jeden prvek nesouhlasí, není možné provést transakci. Přestože jsou všechna bezpečnostní opatření na první pohled neprolomitelná, je tu stále rizikový faktor zneužití.

Kybernetické riziko představuje ohroženost bezpečnosti sítí elektronických komunikací a hrozbu nejenom pro instituce různých odvětví, ale také pro každého jedince, který využívá internet k jakékoliv činnosti. Na druhé straně stojí kybernetická bezpečnost, která se snaží kybernetické útoky odvracet a případně jim zcela zabraňovat. Není to jednorázová implementace bezpečnostních nástrojů, ale nepřetržitý proces, kde se musí opatření pravidelně posuzovat a implementovat opatření nová. Domácí uživatelé by se měli v kyberprostoru chovat obezřetně a v přiměřené míře investovat do zabezpečení svých počítačů i domácích sítí.

Zásadním zlomem bylo pro kybernetickou bezpečnost datum 1. ledna 2015, kdy vstoupil v účinnost zákon o kybernetické bezpečnosti, jehož cílem je zvýšit bezpečnost kybernetického prostoru. Zákon se dotýká pouze vymezeného okruhu osob a orgánů, nicméně pro ostatní subjekty by tento zákon měl sloužit jako vhodná inspirace či metodika.

Přečtením této práce získáte kvalitní náhled na rizika elektronického a bezhotovostního platebního styku a budete tak schopni učinit taková opatření, která Vás ochrání. Cílem této bakalářské práce není odradit od užívání internetu, ba naopak, měli bychom ocenit tento rozmanitý zdroj informací a bránit se hrozbám, jenž na nás na internetu číhají.

2 Cíl práce

Hlavním cílem bakalářské práce je udělat rozbor a vyvodit závěr z nashromážděných výsledků dotazníkového šetření zaměřeného na využívání bezpečnostních prvků a opatření elektronického a bezhotovostního platebního styku, a zároveň posoudit míru informovanosti veřejnosti o jejich rizicích v dané problematice. V rámci vyhodnocování dotazníku bychom chtěli uvést doporučení pro zlepšení informovanosti uživatelů.

Dílčím cílem vedoucím ke zjištění těchto informací je objasnění základních pojmů na téma kybernetické riziko bezhotovostního a elektronického platebního styku a dalších pojmů, jenž jsou s tímto tématem úzce spojené, a které nás budou v práci dále provázet. Při popisování aktuální situace a souvislostí týkajících se tohoto tématu využijeme metodu deskripce.

Mezi další dílčí cíl, vedoucí k naplnění hlavního cíle, řadíme sestavení vhodného dotazníku na základě zvolené metodiky a získání potřebného počtu respondentů daných věkových skupin. V rámci dotazníkového šetření bychom chtěli získat minimálně 400 respondentů reprezentativního vzorku.

Smělým cílem je také poskytnout v této bakalářské práci relevantní informace o aktuálním a vyvíjejícím se tématu, jenž se postupně řeší již několik let, přitom stále není z pohledu běžného uživatele legislativně dostatečně zachyceno.

3 Literární rešerše

V první části práce se zaměříme na teoretický základ, jenž je nutný k pochopení problematiky. Budeme vycházet z domácí i zahraniční odborné literatury, kde identifikujeme nejpoužívanější elektronické platební prostředky a kybernetická rizika spojená s jejich užíváním. Statistické informace budou čerpány z webových stránek bankovních institucí, ČSÚ a EUROSTATU. Zaměříme se i na pojištění kybernetického rizika a popíšeme legislativu, která se k problematice váže. V závěru literární rešerše popíšeme reálné případy útoků na bezhotovostní a elektronické platby v ČR.

3.1 Kybernetické riziko

Společnost se ocitá ve stále větší závislosti na informačních technologiích a dá se předpokládat, že tato závislost bude v budoucnu dále na vzestupu. Tím, že i zájem lidí o danou problematiku vzrůstá, roste s ním i riziko jejich zneužití. Právě toto riziko nazýváme kybernetickým rizikem. Jde o riziko sofistikovaného útoku na informační technologie, jenž může vést k potenciálně velkým škodám. Riziko by se dalo charakterizovat jako činnost, která vzniká s určitou pravděpodobností, a pokud nastane, má pak většinou negativní následky. (Ministerstvo vnitra České republiky, ©2017)

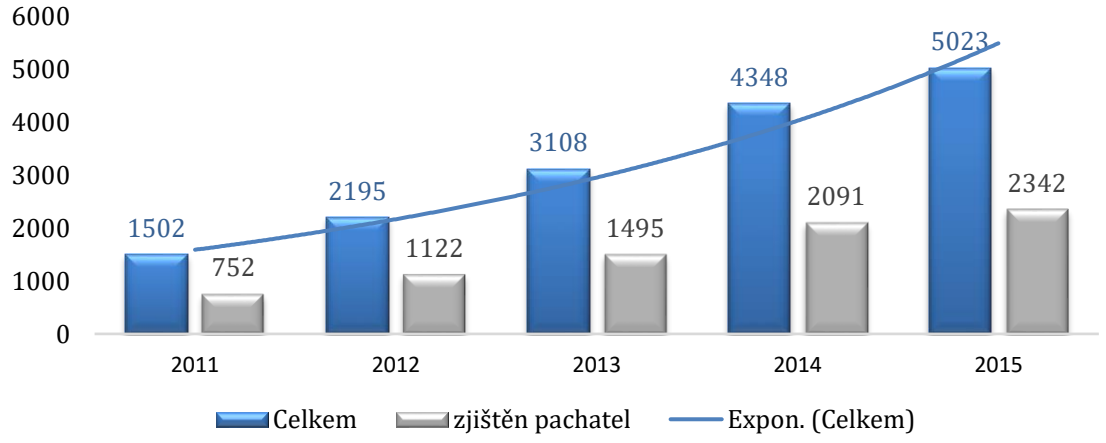
Čím více internet zasahuje do každodenní činnosti obyvatelů, tím vzniká více prostoru pro nové hrozby, které skýtá. Jak se společnost stává na tomto fenoménu závislejší, hrozby nabývají na aktuálnosti a své závažnosti. Útočníkovi může jít jak o citlivé informace uživatelů, tak o zhroucení části sítě. (Janssen, ©2017)

Hrozbu definuje Marťák (2005) jako *„potencionální možnost využití zranitelného místa k narušení integrity, důvěrnosti nebo dostupnosti datových aktiv*.“ Hrozba působí v konkrétním čase, místě a na konkrétní objekty či subjekty. (Dobda, 1998) Mezi projevy kybernetické kriminality řadíme řadu negativních fenoménů s různým stupněm závažnosti. Od kybernetické špionáže, hackerství a DDoS útoků, přes internetové podvody v rámci internetového bankovnictví, krádeže dat z debetních karet a dalších nežádoucích aktivit jako například šíření dětské pornografie, praní špinavých peněz, stalking a internetovou šikanu, až po zneužívání internetu k teroristickým aktivitám spojeným mimo jiné se zveřejňováním návodů na konstrukci výbušnin. (Odbor bezpečnostní politiky a prevence kriminality, 2016) V médiích bývají termíny riziko a hrozba často užívány chybně. Velmi zjednodušeně můžeme říct, že o riziku hovoříme před vznikem jevu a o hrozbě mluvíme při reálném vzniku jevu. Faktickou realizací hrozby je poté konkrétní útok.

Dalším důležitým pojmem je kybernetická kriminalita. Při jeho vymezení musíme brát v úvahu fakt, že se jedná o rozsáhlou oblast trestné činnosti, a že dosud neexistuje žádná univerzální, obecně přijímaná definice, která by rozsah a hloubku tohoto pojmu kompletně postihla. Nabízí se nám tak nepřeberné množství definic, z nichž například podle Jirovského (2007) kybernetická kriminalita znamená *„jakýkoliv čin směřující k narušení nebo zneužití počítače nebo počítačového systému a informací v něm obsažených.“*

Když zabrousíme do historie kybernetické kriminality, můžeme mluvit o třech skutečnostech, které Kolouch (2016) považuje v této oblasti za nejzásadnější. Mezi první řadí propojení čtyř univerzitních počítačů a vytvoření počítačové sítě sloužící ke sdílení dat. Druhou, sestavení prvního osobního počítače společností IBM v 80. letech 20. století a třetí, zpřístupnění Internetu veřejnosti.

Matějka (2002) byl v popisu historie trochu podrobnější a tvrdí, že můžeme první kybernetický zločin datovat k roku 1801, kdy tkadlec Jacguard sestrojil automatizovaný stroj ke tkaní látek. Jeho zaměstnanci si plně uvědomovali rizika tohoto vynálezu, že s obavou před ztrátou míst donutili Jacquarda k přerušení dalšího vývoje. Další čin můžeme směřovat k telefonní komunikaci, kdy skupinka mladých brigádníků telefonní ústředny k sobě spojovala nepatřící hovory. Později se vynález telefonu, prvního prostředku elektronické komunikace, začal využívat i k nelegálním aktivitám, jako například ke komunikaci mezi zločinci. Dalším významným krokem v oblasti technologií bylo datum 14. února 1946, jenž se sestrojil první elektronický počítač jménem ENIAC. Za původ počítačového zločinu můžeme považovat uvedení počítače typu IBM PC na trh. Jednalo se o den, kdy se začala psát historie moderních počítačů, protože byl sestrojen systém propojující svět telefonů a počítačů. Když budeme chtít mluvit o území tehdejšího ČSSR, stojí za zmínku dovezení prvních počítačů na trh koncem 80. let 20. století a připojení země k internetu v roce 1992. Když se zaměříme na následující Obr. 1, již z období novověku, můžeme vidět razantní nárůst kybernetické kriminality. V roce 2015 vzrostl počet trestných činů oproti roku 2011 z 1502 na 5023 tudíž o 3521. Nárůst nám potvrzuje i trendová linie grafu.



Obr. 1 Vývoj kybernetické kriminality v ČR
Zdroj: Dočkalová, 2016

3.2 Zákonný rámec kybernetické bezpečnosti v ČR

Mezi právní předpisy, jenž směřují k posílení důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury můžeme zařadit:

- Zákon č. 40/2009 Sb., trestní zákoník

- Zákon č. 141/1961 Sb., o trestním řízením soudním
- Zákon č. 218/2003 Sb., zákon o soudnictví ve věcech mládeže
- Zákon č. 121/2000 Sb., autorský zákon
- Zákon č. 127/2005 Sb. o elektronických komunikacích
- Zákon č. 480/2004 Sb., o některých službách informační společnosti
- Zákon č. 273/2008 Sb., o Policii České republiky
- Zákon č. 89/2012 Sb., občanský zákoník
- Zákon č. 101/2000 Sb., o ochraně osobních údajů
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce
- Zákon č. 160/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících předpisů (Gřivna el al., 2008)

Zákon o kybernetické bezpečnosti, účinný od 1. 1. 2015 a týkající se pouze vymezeného okruhu právnických osob, orgánů a podnikajících fyzických osob, má za cíl zvýšit bezpečnost kybernetického prostoru. I když se zákon přímo netýká běžného uživatele, na kterého je zaměřena tato práce, mohl by mu posloužit jako inspirace k ochraně informačních a komunikačních systémů před neustále narůstajícími kybernetickými hrozbami.

Za zmínku stojí i právní úprava Evropské unie, z nichž vymezíme pouze ty nejvýznamnější. A to Úmluvu Rady Evropy č. 185 o kyberkriminalitě a dodatkový protokol k ní. Tyto dva dokumenty stanovují základní rámec trestných kybernetických činů a zároveň stanoví prostředky pro odhalování a vyšetřování této kriminality. (Kolouch, 2016)

Mezi instituce dohlížející na kybernetickou bezpečnost řadíme Evropskou agenturu pro informační a síťovou bezpečnost, Evropský CERT a Evropské centrum kyberkriminality. V České republice je to národní CERT a týmy typu CSIRT.CZ, jenž řeší a koordinují řešení bezpečnostních incidentů, provádí školící programy, kooperují se světovou komunitou CERT týmů a spolupracují se subjekty v otázce bezpečnosti v ČR. Národní CERT tým zaštiťuje organizace CZ.NIC. (CSIRT.CZ, 2017a)

3.3 Platební styk

Platební svět je dynamicky rozvíjející se oblastí, kde se i bankám rozšiřují možnosti, jak komunikovat se svými klienty. Čím dál více se tlačí na automatizaci systémů a tím i na jejich rozvoj. Je to z důvodu růstu nákladů na pracovní sílu a možnosti zřízení či ovládání svého účtu odkudkoli a kdekoli.

Mezi základní služby, jenž banky nabízí svým klientům, patří hotovostní a bezhotovostní platební styk. Platební styk vymezuje Kantnerová (2016) jako *„vztah mezi plátcem a příjemcem platby, při němž dochází k převodu finančních prostředků zpravidla prostřednictvím jedné, nebo více bank“.* Hotovostní platební styk můžeme definovat jako platbu probíhající mezi plátcem a příjemcem prostým předáním bankovek či mincí. Na druhou stranu bezhotovostní platební styk probíhá převody mezi

platebními účty plátce a příjemce. Dalším druhem platebního styku je elektronický platební styk, který představuje bezhotovostní formu placení, tudíž vyžaduje i existenci běžného účtu. Tento druh platebního styku je odkázaný na využívání informačních technologií. (Polouček, 2006)

Z hlediska mechanismu provedení transakce a její rychlosti rozlišujeme on-line a off-line platební metody. Vzhledem k tomu, že je pro obchodníka i kupujícího klíčová rychlost provedení transakce, off-line platební metody nejsou již zdaleka tolik atraktivní. Je to převážně kvůli reakční době obchodníka na informaci o zaúčtování transakce, která se může pohybovat od několika hodin až po několik dní. Mezi off-line metody řadíme dobírku, bankovní převod na bankovní účet nebo platbu v hotovosti. Na druhou stranu právě on-line platební metody zajišťují obou stranám rychlé jednání v rámci několika minut a obchodníkovi jistotu, že mu budou příslušné peněžní prostředky zaúčtovány v jeho prospěch. Do těchto metod můžeme zařadit platební karty, platební tlačítka, elektronické peněženky a agregátory platebních metod. (Jansa et al., 2016)

Právní úprava platebního styku je obsažena v zákoně č. 284/2009 Sb., o platebním styku, ve znění pozdějších předpisů. Mezi další právní dokument upravující platební styk můžeme zařadit Zákon o bankách č. 21/1992 Sb. Z evropských předpisů můžeme zmínit Směrnici Evropského parlamentu a Rady 2007/64/ES o platebních službách na vnitřním trhu. (Kantnerová, 2016)

3.4 Platební prostředky

Platební styk uskutečňujeme pomocí elektronických platebních prostředků, kterým se podle Zákona č. 284/2009 Sb., o platebním styku (2009) rozumí *„prostředek vzdáleného přístupu k peněžní hodnotě, při jehož užívání se zpravidla vyžaduje identifikace držitele osobním identifikačním číslem přiděleným vydavatelem nebo identifikace jiným způsobem“.* Platební prostředky budou v následujících podkapitolách popsány.

3.4.1 Platební karty

Platební karta je moderním nástrojem bezhotovostního styku, jenž se stala u mnoha lidí nedílnou součástí každodenního života. Platební kartu popisuje Sdružení pro bankovní karty (©2016) jako „*nástroj sloužící k bezhotovostní úhradě zboží a služeb nebo výběru hotovosti*“.

Průběh bezhotovostního placení platební kartou můžeme rozdělit do tří fází. Na fázi ověření transakce, tzv. autorizaci, která spočívá v kontrole ochranných prvků na kartě a ověření finančního krytí prostřednictvím dotazu (telefonem, přes internet) nebo online, kdy dochází k autorizaci automaticky, většinou po zadání PIN kódu. Další fází je přenos transakce do clearingového systému, probíhající prostřednictví počítačové sítě. Poté proběhne vypořádání platby zúčtovací bankou na základě výstupu z clearingového systému. Jednotlivé banky následně zatíží či kreditují účty svých klientů. (Máče, 2006)

V případě, kdy nemůžeme za zboží či službu zaplatit bezhotovostně, musíme si peníze vybrat na bankovní pobočce, v obchodě či prostřednictvím bankomatu. S první myšlenkou bankomatu přišel Skot John Shepard Baron, který nebyl spokojený s úředními hodinami banky a tak začal přemýšlet o způsobu, jak mít peníze k dispozici 24 hodin denně. (Juřík, 2001)

Platební karty podle vydávající asociace

Naprostá většina vydaných karet v České republice nese logo VISA nebo MasterCard. Akceptace karet probíhá na téměř podobném principu. Mimo značku karty rozlišujeme také její model. Čím vyšší model karty, tím jsou větší požadavky na bonitu klienta. Kromě výše uvedených společností můžeme řadit k nejznámějším světovým kartovým společnostem Diners Club, JCB (Japan Credit Bureau), AmEx (American Express) či Discover Financial. (Kantnerová, 2016)

„Mezi náležitosti a ochranné prvky přední strany platebních karet MasterCard a VISA patří:

1. *Logo MasterCard či VISA*
2. *Hologram znázorňující u MasterCard rozvinutou polokouli a u VISA letící holubici*
3. *Název, většinou i logo vydavatele platební karty*
4. *Číslo platební karty začínající číslicí 5 u MasterCard, 4 u VISA*
5. *Jméno držitele karty*
6. *Období platnosti platební karty*
7. *Pod UV lamou viditelná písmena MC u MasterCard, letící holubice nebo písmeno V u VISA*
8. *Nad číslem platební karty je umístěn čip" (KB, ©2011)*

„Mezi náležitosti a ochranné prvky zadní strany patří:

1. *Magnetický proužek*
2. *Podpisový proužek s*
   - *podpisovým vzorem držitele karty,*
   - *posledním čtyřčíslím čísla Platební karty doplněným o tři kontrolní číslice, tzv. CVC2 u MasterCard a CVV2 u VISA.*
3. *Hologram znázorňující rozvinutou polokouli u MasterCard a letící holubici u VISA" (KB, ©2011)*

Platba kartou v síti Internet

Platbu platební kartou na internetu můžeme řadit mezi poměrně bezpečnou metodu placení. Obchodník využívá buď zakódovaný přenos údajů o platební kartě, tzv. *SSL* nebo zabezpečení *3D Secure protokol*, kde je zákazník přesměrován přímo na webové rozhraní banky. Mezi hlavní výhody 3D Secure můžeme zařadit nepřístupnost údajů o naší platební kartě obchodníkovi, který je pouze informován o provedení platby a může tak odeslat zboží.

3D Secure protokol je na stránkách znázorněn logem Verified by Visa nebo MasterCard SecureCode. Díky mezinárodní platnosti karet mohou klienti platit i na mezinárodních portálech.

Pro platby kartou je třeba mít aktivní možnost plateb po internetu, kterou sjednáme u své banky. Kvůli bezpečnosti se volí i *denní finanční limit* pro internetové transakce. Při internetové platbě prostřednictvím karty systém požaduje *číslo karty, datum konce platnosti karty* a kontrolní hodnotu *CVV2/CVC2*, jenž nalezneme na zadní straně platební karty. Následně nám od banky přijde potvrzující jednorázový *SMS kód* na telefonní číslo, uvedené ve smlouvě. Pro ještě větší ochranu je možné si sjednat i pojištění, které se nemusí týkat pouze plateb na internetu (více o pojištění v kapitole 3.6). (Matyáš et al. 2008)

Neměli bychom opomenout i na skutečnost, že ne každý obchodník jedná se svými zákazníky poctivě. Podvodníci jsou vynalézaví a Internet jim dává řadu možností, jak lidi obelstít. Proto bychom měli věnovat pozornost samotnému *výběru obchodníka*. Asociace pro elektronickou komerci (2013) radí nakupovat u seriózních e-shopů s logem APEK či SAOP. Pokud obchod nemá na svých stránkách tyto loga, a s obchodníkem nemáme předchozí zkušenosti, je vhodné si o něm přečíst reference či využít platby pomocí dobírky.

Důraz bychom měli klást i na výběr *prohlížeč*e, jenž o nás může mnohé prozradit. Podle stránek vývojáře Robina Linuse ([b.r.]) na nás může náš prohlížeč prozradit polohu (aniž bychom měli spuštěné GPS), verzi operačního systému, informace o hardwaru počítače či výpis sociálních sítí, ke kterým jsme v prohlížeči právě přihlášeni. Většina prohlížečů obsahuje funkci bezpečné prohlížení, fungující na principu přenášení informace o podezřelých webech mezi prohlížečem a servery. Prohlížeč automaticky prověřuje zabezpečené webové certifikáty, stahuje seznamy podvodných a škodlivých stránek (aby nám mohl blokovat přístup) a provádí další bezpečnostní operace, jenž slouží ku prospěchu naší bezpečnosti. (Google, 2016)

Strašákem by mohly být i soubory cookies. které stránce dovoluji, aby si pamatovala uživatelské nastavení. Díky cookies souborům mizí anonymita a my přicházíme o soukromí. Obavy z cookies záleží na tom, zda se jedná o primární soubor, nebo soubor cookie třetí strany. Primární soubor cookie je ten, který se do počítače uloží při navštívení konkrétní webové stránky. Na druhou stranu cookies třetích stran ukládá jiná stránka než ta, na které se právě nacházíte. Prohlížeče volbu povolení cookies třetích stran nedoporučují. (MCCarthy a Weldon-Siviy, 2013)

I přestože mezi doporučené bezpečnostní pokyny každé banky patří informace nevyužívat k platbám veřejný *počítač* či veřejnou lokální bezdrátovou *síť*, z průzkumu Intelu (2015) vyplynulo, že mimo domov, na cestách či na dovolené, kdy je

veřejná Wi-Fi síť využívaná nejvíce, zadává své osobní údaje včetně hesel, PIN kódu a údajů o platební kartě čtyři z deseti respondentů v ČR. Společnost Intel tvrdí, že každý kdo využívá k platbě internetové připojení zdarma, by měl vyhodnotit důvěryhodnost konkrétního poskytovatele této služby, protože u nedůvěryhodných provozovatelů wi-fi hotspotů se uživatel vystavuje riziku zneužití osobních údajů a nepříjemnostem vzniklých neoprávněnou osobou.

Bránit počítač od nezvaných hostů, kybernetických útočníků, může i kvalitní *antivirus* sloužící k identifikaci, odstraňování a eliminaci škodlivého softwaru. Je potřeba aktualizovat programy a zapínat antivirové kontroly. V neposlední řadě by si měla každá domácnost v rámci bezpečnosti nainstalovat bránu *Firewall*, jenž je prvním krokem k ochraně počítače před útoky ze sítě. Firewall je něco jako bezpečnostní brána oddělující provoz mezi dvěma sítěmi, naší domácí a internetem. Firewall propouští data podle určitých pravidel a brání tak před neoprávněnými průniky do sítě bez souhlasu uživatele.

Další cennou radou je kontrolovat si při platbě *adresní řádek*. Bezpečnou stránku poznáme jednak podle URL, která začíná protokolem https://, nikoli pouze http://, a také pomocí malé ikonky zámku. Při platbě se zabezpečením 3D Secure jsme upozorněni bankou těsně před zaplacením, že si máme ověřit, že se nacházíme na konkrétní, pravé stránce, a že zelená ikonka zámečku indikuje bezpečné spojení. (Mozilla, 2017)

3.4.2 Platební prostředky bezkontaktní platby

Bezkontaktními platbami nazýváme takové platby, kde není nutný fyzický dotek mezi platícím nástrojem a platebním terminálem. Velkou výhodou, oproti jiným alternativám placení, je rychlost bezkontaktní platby. V případě uskutečnění transakce stačí mít na přední straně platebního prostředku specifický symbol pro bezkontaktní platby a můžeme jej v tu ránu začít používat. Realizovat platbu lze u všech prodejců, jenž mají platební terminál se symbolem pro přijímání bezkontaktních plateb. Obchodní místa, jenž dané platby podporují, jsou označeny logy, zobrazenými na Obr. 2 a Obr. 3.

Obr. 2 Paypass, PayWave
Zdroj: Visa, ©2017

Obr. 3 Mezinárodní označení obchodního místa podporující bezkontaktní platby
Zdroj: Visa, © 2017

Bezkontaktní platba do výše 500 Kč funguje na principu přiložení prostředku k bezkontaktní čtečce, tudíž fyzicky nedává držitel nástroj z ruky. Je tím zaručena určitá forma bezpečnosti. Platby nad 500 Kč obvykle vyžadují následnou autorizaci pomocí *PIN*u. Technologie bezkontaktní platby se primárně využívá v rámci platební karty, nicméně je ji možné taky zabudovat do jiných nosičů, jako jsou klíčenky, hodinky, mobilní telefony, nálepky či náramky. Když se na technologii podíváme z pohledu obchodníků, můžeme říct, že pro ně zavedení znamená především získání konkurenční výhody. Navíc platby urychlují dobu obsluhy a krátí čekání u pokladen.

Platba platební kartou

Nejpoužívanějším platebním nástrojem je bezpochyby bezkontaktní platební karta. Mezi nejznámější produkty karetních společností patří MasterCard® PayPass™ a Visa payWave™. Komunikace je zajištěna pomocí RFID (Radio Frequency Identification), kdy vysílač periodicky vysílá do okolí elektromagnetické pulsy. Jakmile se v blízkosti objeví pasivní RFDI čip, využije přijímanou energii k nabití svého napájecího zařízení a odešle odpověď zpět k vysílači. (KartyvBezpeci.cz, [b.r.]) Díky těmto technologiím se transakce urychlí pouze na 5 sekund.

Z průzkumu společnosti MasterCard vyplynulo, že bezhotovostní platební karty používalo v roce 2016 88 % Čechů. Vůči roku 2015 můžeme mluvit o 10% nárůstu v používání bezkontaktních plateb. U lidí se změnil i postoj k bezkontaktní platbě, uvědomili si totiž její benefity. Zatímco v roce 2015 hradili kartou nákup až v průměru od 1400 Kč, podle průzkumu za rok 2016 se hranice snižuje na 1000 Kč. Průzkumem také bylo potvrzeno, že využití karet roste se vzděláním a výší příjmů zákazníků. (Bubák a Dusová, 2017)

Platba mobilním telefonem s technologií NFC

Banky v ČR odstartovaly ve spolupráci se společnostmi Visa a MasterCard bezkontaktní platby prostřednictvím mobilního telefonu. Tyto platby používají technologii HCE (Host Card Emulation – uložení emulované platební karty v zabezpečeném prostřední vydavatele karty se vzdáleným přístupem k ní prostřednictvím mobilního zařízení vybaveného technologií NFC). Technologii mohou využívat klienti s NFC a nainstalovanou aplikací konkrétní banky. Uživatel si může také kartu zobrazit na ploše telefonu pomocí tzv. widgetu. Bezpečnost je zajištěna požadováním *PIN kód*u při překročení limitu transakce.

Mezi další bezpečnostní prvek platby mobilním telefonem s technologií NFC můžeme řadit uzamčení telefonu heslem. Zabezpečení mobilního telefonu *heslem* by

se některým mohlo zdát jako zbytečné, avšak jedinci využívající mobilní bankovnictví či platbu pomocí NFC by se nad touto možností zabezpečení měli pozastavit. Připadat v úvahu by mohl čtyřmístný číselný pin. I přestože není považován za silnou ochranu, útočníka přinejmenším odradí, protože nemusí mít dostatek času na vyzkoušení všech možných kombinací. V technologicky pokročilejších smartphonech stojí za to používat zabezpečení pomocí biometrických údajů, jako je například otisk prstu.

Pokud se na zabezpečení mobilního telefonu podíváme podrobněji, mohli bychom diskutovat i o zabezpečení SIM karty *PIN kód*em. Jedná se o čtyřmístný kód, jenž zadáváme vždy při zapnutí telefonu. Útočník má pak pouze 3 pokusy, než se mu SIM karta zablokuje a nedostane se tak k manipulaci s telefonním číslem.

Platba čipovou nálepkou

Za další zvrat bezkontaktního placení, blížící se k předmětům denního využití, můžeme považovat čipovou nálepku. Jedná se o miniaturu platební karty, kterou můžeme nalepit na zadní stěnu mobilního telefonu, přívěsek na klíče či další předměty dle naší libosti. Jde o formu placení, která zcela jistě nahrazuje platební karty. Jedinou nevýhodu můžeme vidět v nemožnosti vybírání peněz z bankomatu, který nemá bezkontaktní možnost výběru. Nálepky umožňují provádět platby do 500 Kč bez nutnosti zadávat PIN. Bezpečnost této technologie je tedy obdobná jako u bezkontaktní platby kartou. (Kohoutová, 2014)

Wareables – platba nositelnou elektronikou

Možnost, jak jít kupředu v moderních metodách placení, v sobě skýtá wearables, tzv. nositelná elektronika. Jsou to zařízení, jenž jsou připravena pomáhat lidem usnadnit si pomocí technologií běžný život. Na rozdíl od běžné přenosné elektroniky je zde důležitý aspekt v možnosti upevnění zařízení na tělo. V České republice si zatím drží první pozici v užívání chytré hodinky. Nicméně pokud nahlédneme mimo naše území, nabízí se nám možnosti platby pomocí platebního prstenu, náramku, oblečení či zabudovaného čipu v těle. (Wareable, ©2014 – 2017)

Již před několika lety společnosti Apple a Android přišly na trh s možností platit *chytrými hodinkami*. Prvním představitelem bankovních funkcí pro chytré hodinky byla v ČR Komerční banka, jež představila aplikaci v únoru 2016. Nicméně momentálně již nabízí smartbanking v hodinkách téměř každá banka. Hodinky umožňují zjistit aktuální zůstatek či zobrazit informace o příchozích i odchozích platbách. Operační systémy sloužící k využívání bankovnictví v hodinkách se nazývají Apple Watch a Android Wear. (Komerční banka, 2016)

Společnost KERV přišla na trh s prvním bezkontaktním *platebním prstenem*, jenž používá totožnou technologii jako bezkontaktní platební karta. Jelikož jsou prsteny spojeny s certifikací MasterCard, podporují je miliony terminálů po celém světě. Z toho důvodu můžeme použít prsten k provedení platby na jakémkoliv místě, který přijímá MasterCard bezkontaktní platby. V případě koupě je nutná pouze bezplatná aktivace prstenu a propojení tak s MasterCard účtem. Žádné další poplatky

se nehradí. Jedná se o prsten, který je dostupný pouze v Anglii, avšak plánuje se i rozšíření prodeje do USA, Austrálie a samozřejmě i Evropy. (Kerv, 2017)

O další moderní formě placení můžeme mluvit v souvislosti se společností Jawbone, zabývající se výrobou chytrých náramků. Ta přišla na trh s bezkontaktní formou placení pomocí stylových *náramků*, již mají v sobě zabudovaný NFC čip, který ovšem mohou využívat pouze držitelé karty American Express. Kdy se tato vymoženost dostane do České republiky, se zatím neví. (Smrž, 2015)

Pro někoho, kdo není zastáncem módních doplňků ve stylu prstýnků, náramků či hodinek, přišla firma Lyle & Scott a Barclays s návrhem *bundy* se zabudovaným NFC čipem. Čip je skryt v manžetě rukávu a propojen s účtem uživatele. Poté stačí pouze zaplatit přejetím rukávu nad platebním terminálem kdekoliv na světě. Barclays je kompatibilní s jakýmkoliv účtem Visa nebo Mastercard a lze ji pořídit za 150 liber. Výrobci samozřejmě mysleli i na to, že bundu nelze nosit celý rok, proto můžeme čip v manžetě přeměnit na náramek a pokračovat tak v placení. (Nield, 2015)

Za zmínku stojí i moderní platební technologie ve formě *čipu implantovaného pod kůží* ruky, jenž si v roce 2016 nechalo v České republice vpravit do těla asi 30 lidí. Jedná se o úložiště dat ve formě skleněné kapsle o velikosti 12 x 2 milimetry, které funguje díky NFC čipu a anténě. V tuto chvíli jde o technologii, kterou lze využívat jednak k placení v místech, kde je akceptována virtuální měna bitcoin či k přihlašování se do počítače. Manažer inovací české Mastercard tvrdí, že zatím neuvažují o nabídce této technologie klientům. Napojit čip na platební kartu se tedy blízké době neplánuje. Z toho tvrzení můžeme vyvodit závěr, že čip zůstane menšinovou záležitostí a nenajde tak ještě nějakou chvíli komerční uplatnění. (Černý, 2017)

3.4.3 Elektronické peněženky

Elektronická peněženka je platební instrument v podobě čipové karty, sloužící k platbám malých částek bez zadávání PINu. Tato karta funguje na podobném principu, jako kredit u mobilního telefonu. Jednoduše stačí peněženku dobít na pobočce kterékoliv banky bez potřeby mít zřízený běžný účet. Obrovský potenciál v sobě skrývají tzv. virtuální elektronické peněženky, mezi něž řadíme PayPal. Na rozdíl od běžných platebních nástrojů se PayPal nezajímá pouze o převod finančních prostředků, ale také o doručení a kvalitu zboží. Pokud se v případě problému nepodaří dohodnout s prodejcem, můžeme spor předat přímo PayPalu. (Finanční poradenství online, ©2012 – 2017)

Vzhledem k tomu, že do e-peněženky nabíjíme pouze tolik peněz, kolik uznáme za vhodné, je zde zajištěna určitá bezpečnost v podobě omezení *částky* případného napadení. Dalším znakem bezpečnosti je fakt, že nikde neuvádíme žádná citlivá data, jako je to například u platby platební kartou v síti Internet. Další bariéru zneužití představuje nastavení *limit*u *transakce*, který při překročení požaduje autorizaci pomocí mobilního telefonu. (Hájková, 2014)

Bezpečnostní prvky jsou jinak téměř shodné s platbou v síti Internet. Mluvíme tedy o výběru vhodného *zařízení* pro platbu, bezpečné volbě *prohlížeč*e i *sítě* a používání *antivir*u, jenž automaticky a průběžně aktualizujeme.

3.4.4 Homebanking a internetové bankovnictví

Homebanking funguje na principu propojení osobního počítače klienta s počítačem banky pomocí speciálního programu. Výhodou je provádění téměř všech bezhotovostních operací jednoduše, bezpečně a spolehlivě 24 hodin denně. Nevýhodou této služby je licenční vázanost na jeden počítač. (Máče, 2006)

Na rozdíl od služby Homebanking, kde je zapotřebí instalace speciálního programu, k internetovému bankovnictví je potřeba mít pouze počítač, připojený na internet, a internetový prohlížeč. (Máče, 2006)

Ochranný systém internetového bankovnictví lze přirovnat ke stavebnici. Systém ochrany se skládá z několika základních a na sobě nezávislých prvků, a jakmile třeba i jediný prvek chybí nebo nesouhlasí, nelze bankovnictví považovat za bezpečné. Bezpečnost internetového bankovnictví je založena především na identifikaci banky, identifikaci klienta a na zabezpečení přenosu dat. Komunikace klienta s bankou bývá zabezpečena standardním protokolem *SSL* (HTTPS). Autentizace uživatele u homebankingu a internetbankingu využívá autentizační systémy, které využívají *uživatelské jméno a heslo*, jenž lze považovat za základní způsob ověření identity uživatele. Nicméně tento způsob ověření je vhodné kombinovat s další autentizací jako je například *SMS kód, PIN kód či certifikát*. (Matyáš et al. 2008) Aby banky udržely peníze v bezpečí, nastavují maximální *denní limit* pro odchozí platby. Tento limit lze samozřejmě na účtu uživatele spravovat, nicméně doporučuje se mít limit nízký, a v případě potřeby si ho výjimečně na den zvýšit.

Mimo jiné bychom si měli také chránit své zařízení, které využíváme při komunikaci s internetovým bankovnictvím. Česká spořitelna uvádí základní pravidla, jenž by měl dodržovat v rámci bezpečnosti každý uživatel:

1. *Pravidelně aktualizujte svůj operační systém a internetový prohlížeč* – instalujte bezpečnostní záplaty a balíčky, které výrobce doporučuje.
2. *Instalujte si aplikace výhradně z oficiálních obchodů* – Nikdy neinstalujte do svých počítačů programy ze zdrojů, které nemáte prověřeny. Při instalaci aplikací do svých mobilních telefonů, stahujte aplikace pouze z oficiálních obchodů (App store, Google play a Windows phone strore).
3. *Nepřipojujte ke svému počítači neznámá paměťová média* (USB flash disky, CD, DVD) – Taková média mohou být infikovaná a jejich připojením dojde k instalaci škodlivého softwaru, díky kterému může útočník získat přístup k vašemu počítači nebo síti, ve které je připojený. (Česká spořitelna, ©2017a)

S ochranou zařízení souvisí i rada banky nepřihlašovat se do internetového bankovnictví z kaváren či jiných veřejných míst, ale *přihlašování se* výhradně *ze svého počítače*. Než se do svého bankovnictví přihlásíme, je nutno zkontrolovat *adresní řádek* se správnou adresou banky. Důležitý je také *obrázek zámečku* v adresním řádku, který by měl po kliknutí zobrazit informace o certifikovaném zabezpečení dané služby. (MONETA Money Bank, ©2017)

Jak si můžeme v následující tabulce všimnout, nárůst počtu uživatelů v používání internetového bankovnictví je během 6 let opravdu znatelný. V ČR můžeme vidět až 28% nárůst. Dalším faktem je, že ČR byla v roce 2010 pod průměrnou úrovní

států EU, kdy se rozdíl v počtu jedinců využívajících internetové bankovnictví lišil o 13 %.

Tab. 1 Jednotlivci využívající internetové bankovnictví v letech 2010–2015

	2010	2011	2012	2013	2014	2015	2016
ČR (%)	23	30	34	41	46	48	51
EU (%)	36	36	40	42	44	46	49

Zdroj: Eurostat, 2017

Porovnáme-li výsledky Eurostatu se zprávami o činnosti dvou největších bank České republiky, tak ČSOB uvádí, že k datu 30. 6. 2016 až 55,14 % jejich klientů využívá internetové bankovnictví. (ČSOB, 2016) Banka je tedy v tomto ohledu nad průměrem bank České republiky. Na druhou stranu Česká spořitelna ve své zprávě sděluje, že ze 4,74 mil. klientů, je pouze 36 % (1,71 mil.) aktivních v jejich internetovém bankovnictví. (Česká spořitelna, 2016)

Rychlá platební tlačítka

Rychlé platební tlačítko nahrazuje zadávání údajů z platební karty do online formulářů internetových obchodů. Vyžaduje však, aby měl plátce zřízené internetové bankovnictví u své banky a obchodník uzavřenou smlouvu s toutéž bankou o poskytování rychlého platebního tlačítka. Kliknutím na odkaz ve formě grafického symbolu dané banky bude zákazník přesměrován do svého internetového bankovnictví, kde má již předvyplněné veškeré potřebné údaje k platbě. Příkaz pouze potvrdí či provede vyšší ověření *SMS* nebo *certifikátem*, a bude následně přesměrován zpět do e-shopu. (Jansa et al., 2016)

3.4.5 Platební agregátory

Platební agregátor neboli platební brána, je založena na poskytování platebních metod v jednom balíčku, který poskytují platební agregáty na základě smlouvy obchodníkům. Zákazníci tak získají možnost z co nejširšího spektra platebních metod vybrat si tu, která jim nejvíce vyhovuje. Může se jednat o platbu pomocí internetového bankovnictví, platební karty, peněženky, SMS apod.) Jakmile platební agregátor obdrží informaci o autorizaci transakce, předá zprávu obchodníkovi, který může okamžitě odeslat zboží, aniž by musel čekat na fyzické peníze. Veškerá komunikace mezi platební bránou a platícím klientem je vždy zabezpečena pomocí *SSL* a transakce platební kartou jsou dle výše částky chráněny zadáním osobního *PIN*u. Tato on-line metoda splňuje i všechny bezpečnostní standardy. (GoPay, ©2016) Mezi nejznámější platební brány řadíme GoPay a PayU.

3.4.6 GMS banking a telefonní bankovnictví

Dalšími, v dnešní době již ne tak moderními bankovními komunikačními kanály, jsou telefonní bankovnictví a GMS banking. I když se tyto platební prostředky hojně

nevyužívají, určitě stojí za zmínku. Phonebanking je založen na komunikaci s bankou prostřednictvím automatického hlasového systému (IVR) či telefonního bankéře, což považujeme za osobnější variantu. (Přádka a Kala, 2000)

Telefonní systém provádí jednoduché operace na základě menu, po kterém se klient může pohybovat prostřednictvím tlačítek na telefonu. Pokud menu nenabízí žádnou z námi požadovaných služeb, přepojí nás na operátora, který je schopný řešit složitější požadavky či vzniklé problémy. (Přádka a Kala, 2000)

Vstupu do systému přechází autentizace uživatele, kde se ověřuje uživatelské *jméno a heslo* či *PIN* přidělené při zřízení služby. Může se jednat o jednorázová hesla, kde každé slouží jen pro jednu bankovní operaci. K ověření identity může banka využít *mobilního či elektronického klíč*e, či znalost *identifikačních údajů* vlastníka účtu. (Matyáš el al. 2008)

GMS banking je bankovní služba, založená na ovládání běžného účtu prostřednictvím mobilního telefonu. Jednou z možností je odesílání přesně nadefinovaných SMS zpráv s požadavky k získání informací nebo provedení příkazů. Banka odesílá automaticky nebo na vyžádání odpovědi SMS zprávou obsahující požadovanou informaci, tyto informační služby jsou nadefinované klientem. (Máče, 2006)

Využívat bankovní služby můžeme také pomocí GSM SIM Toolkit, k čemuž je zapotřebí využívat služeb operátora, být klientem banky nabízející tuto službu, mít mobilní telefon podporující technologii SIM Toolkit a vlastnit speciální SIM kartu pro bankovní služby. Zašifrovaná zpráva, vytvořená po zadání všech požadovaných údajů v aplikaci, může být rozšifrována pouze speciálním softwarem v bance. (Přádka a Kala, 2000)

Další služba, jež stojí za zmínku, je služba WAP (Wireless Apllication Protocol), která je založená na kombinaci telefonního a internetového bankovnictví. Umožňuje uživatelům přístup na WAP stránky banky, jenž jsou speciálně upravené pro displeje mobilních telefonů. (Máče, 2006)

3.4.7 Smartbanking

Nicméně pamatování si či stálé nošení u sebe struktury textových zpráv není zrovna pohodlné. Totéž můžeme říct o standardu GSM SIM Toolkit a službě WAP, jež se stávají také zapomenutými. Tyto služby byly nahrazeny modernějším a pohodlnějším způsobem spravování našeho účtu – smartbankingem.

Smartbanking umožňuje rychlý, moderní a snadný přístup k financím odkudkoliv pomocí chytré bankovní aplikace vyvinuté speciálně pro smartphone telefony, tablety či hodinky. Aplikace je vyvinuta pro mobilní operační systémy iOS, Android i Windows Phone. Banky nabízí i možnost QR kódu, který nás automaticky rozpozná a přesměruje nás do příslušného obchodu. (ČSOB, ©2016)

Každé nové zařízení, na kterém chce klient využívat aplikaci mobilního bankovnictvím, musí propojit se svým internetovým bankovnictvím, a to za použití *přihlašovacího jména, hesla a potvrzovacího SMS kódu*. Dalším opatřením, vedoucím ke snížení rizika útoku je *počet zařízení*, na které můžeme bankovnictví propojit. Neměli bychom zapomínat na kvalitní antivirový program s pravidelnými aktualizacemi. Přihlášení do mobilní banky se liší jednotlivými bankami. Některé využívají *hesla*,

některé stejných *přihlašovacích údajů*, jako do internetového bankovnictví. Přístup a podpis plateb je chráněn pomocí *PIN či SMS kód*u. Dalším bezpečnostními prvky jsou *limit*, který částka poslaná přes Smartbanking nesmí překročit a *odhlášení při nečinnosti* (konkrétní nastavení délky nečinnosti se liší jednotlivými bankami). Aplikace je propojena přímo s mobilním telefonem klienta, přičemž v mobilu nejsou ukládány žádné citlivé informace.

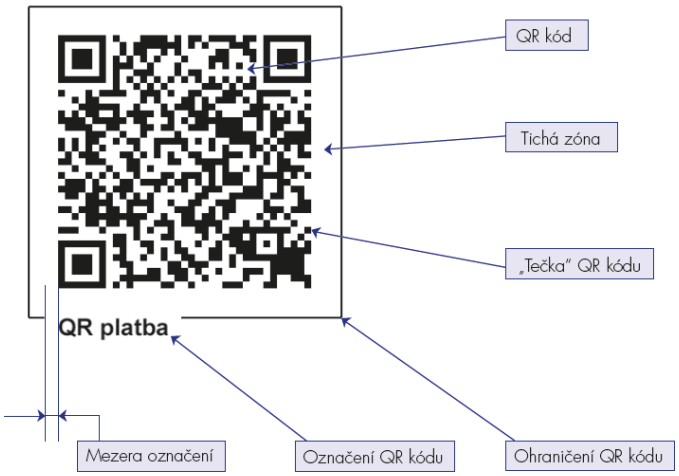
Nicméně i přes všechny tyto kvalitní formy zabezpečení společnost Gartner očekává, že v roce 2017 bude připadat na tři útoky na mobilní zařízení jeden útok na běžný desktopový počítač. (Čečelský, 2016)

QR platba

QR kód vychází z anglického slova „*Quick Response*“, tedy kód rychlé reakce. Slouží jako nástroj pro automatizované čtení a sběr dat a dokáže zakódovat mnohem větší množství informací, než klasický čárový kód. S QR kódem se můžeme setkat i v oblasti bankovnictví, kde již nebudeme muset složitě přepisovat číslo účtu, variabilní symbol a další údaje o platbě. QR platba slouží k usnadnění vyplňování platebního příkazu v mobilní bankovní aplikaci. Vyfocením QR kódu z faktury chytrým telefonem se platební příkaz v aplikaci vyplní automaticky. Sami údaje vůbec nemusíme vypisovat, pouze je zkontrolujeme a odešleme standardním způsobem do banky. Samozřejmostí je také fakt, že si můžeme vygenerovat svůj platební QR kód. (QR Platba, ©2017)

Nicméně společnost AVG Technologies (2012) upozorňuje uživatele, že každý systém může být napaden, a tudíž i QR kódy. Neměli bychom proto skenovat ty neověřené, jenž nás mohou přesměrovat na stránky s nevyžádaným obsahem a stáhnout tak nebezpečný malware, který bude bez našeho vědomí ovládat náš telefon.

Na Obr. 4 můžeme vidět grafické provedení QR kódu. QR platbu na platebních dokumentech poznáme právě podle grafického provedení. Základem je černá linka kolem samotného QR kódu, prázdná oblast kolem QR kódu a označení „QR platba“ v pravé dolní části. (QR Platba, ©2017)



Obr. 4 QR kód
Zdroj: QR PLATBA, © 2017

3.4.8 Autorizace bankovních operací

Jakákoliv operace s finančními prostředky je považována za citlivou a důvěrnou informaci, protože přitahuje pozornost různých útočníků, jenž se chtějí obohatit na úkor ostatních. Vzhledem k pokroku doby jsou kriminálníci díky mnohým bezpečnostním systémům vystaveni poměrně velkému riziku odhalení, protože si společnosti dávají záležet na způsobu autentizace a autorizace finančních transakcí.

V dnešní době se již nesetkáme s autorizací pomocí podpisu. Tento způsob autorizace platební karty je nyní nahrazován zaváděním EMV karet s čipem. Nevýhodou této autorizace je nemožnost grafologické kontroly ze strany obchodníka či skutečnost, že se lze snadno podpis naučit. Na druhou stranu je to rychlý a jednoduchý způsob provedení platby. (Matyáš et al., 2008)

Na druhou stranu autorizace pomocí PINu je zcela převládající formou autorizace, při níž omezujeme počet pokusů, které máme k dispozici pro uhádnutí hodnoty PINu. Pokud nezadáme správně číslice, systém PIN zablokuje a na odblokování musíme využít kontakt se zákaznickým centrem. Mezi klady autorizace pomocí PINu patří jednoznačné rozhodnutí o správnosti či nesprávnosti autorizace. (Matyáš et al., 2008)

Dalším způsobem je autorizace plateb pomocí elektronického podpisu na bázi PKI, kde se *„při placení vytvoří elektronický převodní příkaz, který se standardním způsobem elektronicky podepíše. Po dokončení příkazu je odeslán do banky, kde se ověří likvidita účtu a provede se verifikace transakce“*. (Matyáš et al., 2008)

Metoda autorizace, jenž převládá při platbě na internetu je autorizace pomocí SMS jednorázového hesla. Předpokladem je pouze to, že klient vlastní mobilní telefon.

Mezi nejdražší a nejsložitější formu autorizace řadíme jednoznačně autorizaci pomocí biometriky, která využívá jedinečných tělesných znaků pro identifikaci

osoby. Je to metoda využívaná již z historie, kdy se lidé rozpoznávali podle vzhledu tváře či otisku dlaní v jeskyních. Nicméně s rozvojem technologií se stalo biometrické rozpoznávání automatizovaným. Mezi výhody patří skutečnost, že biometrické znaky se během života nemění, nelze je zapomenout a není nutné si pamatovat složitá hesla. (Kocman a Lohniský, 2005) Přestože ve srovnání s jinými bezpečnostními prvky je biometrické identifikační údaje těžší zkompromitovat, nemusejí být tyto relativně nové metody nejlepším řešením. Pokud se totiž útočníkům podaří najít způsob, jak je ukrást či podvrhnout, bude těžší je změnit nebo zaktualizovat.

Zabezpečení platebních prostředků je základním prvkem ochrany platebního účtu a je na uživateli, jak důkladně bude dodržovat bezpečnostní pravidla doporučená jeho bankou. Nicméně je potřeba říct, že každý typ zabezpečení lze podrobit útokům, ale metody autorizace či jejich kombinace tyto hrozby snižuje.

3.5 Projevy kyberkriminality

Podle Koloucha (2016) *„v podstatě nejde nalézt takovou oblast lidské činnosti, kde by se přímo nebo zprostředkovaně nevyužívala výpočetní technika, resp. informační systém nebo informační či komunikační technologie“*. Proti těmto technologiím může být veden útok, jehož efekt se může projevit jako malá nepříjemnost způsobená uživateli, či velká finanční ztráta a výpadek důležité funkce společnosti. Jakmile útočník pronikne do informačního systému, může ho nepozorovaně zneužívat dlouhou dobu. (Jirovský, 2007)

Podle světového ekonomického fóra jsou kybernetické útoky nejzávažnějšími riziky budoucnosti. Právě 36 % úspěšných útoků se odehraje ve chvíli, kdy se osoba připojí na svůj účet prostřednictvím veřejné Wi-Fi sítě, a 76 % útoků připadá na malware, který nezachytí antivirová ochrana. (Duračinská, 2016)

Vzhledem k rozvoji informačních technologií a různorodému pohledu na kybernetický útok, není stále tento útok přesně nadefinován. Nicméně obecně můžeme říct, že jde o zneužití počítačových systémů, které mohou mít za následek ohrožení dat a krádež identity a jenž vedou k počítačové kriminalitě. (Janssen, ©2017)

Na útočníky se můžeme dívat ze dvou hledisek. Jednak je můžeme považovat za vynalézavé a obzvlášť chytré jedince, kteří perfektně ovládají programovací techniky, nebo za počítačové vandaly a zločince, jenž chtějí na počítačovým systém zaútočit se zlými úmysly. Podle logické polohy útočníka vzhledem k napadenému systému rozlišujeme vnitřního útočníka (připojeného do vnitřní počítačové sítě), vnějšího útočníka (osobu, která musí překonat nástrahy, připravené správcem sítě) a celý svět, což je nejnebezpečnější druh útočníka. (Doseděl, 2004)

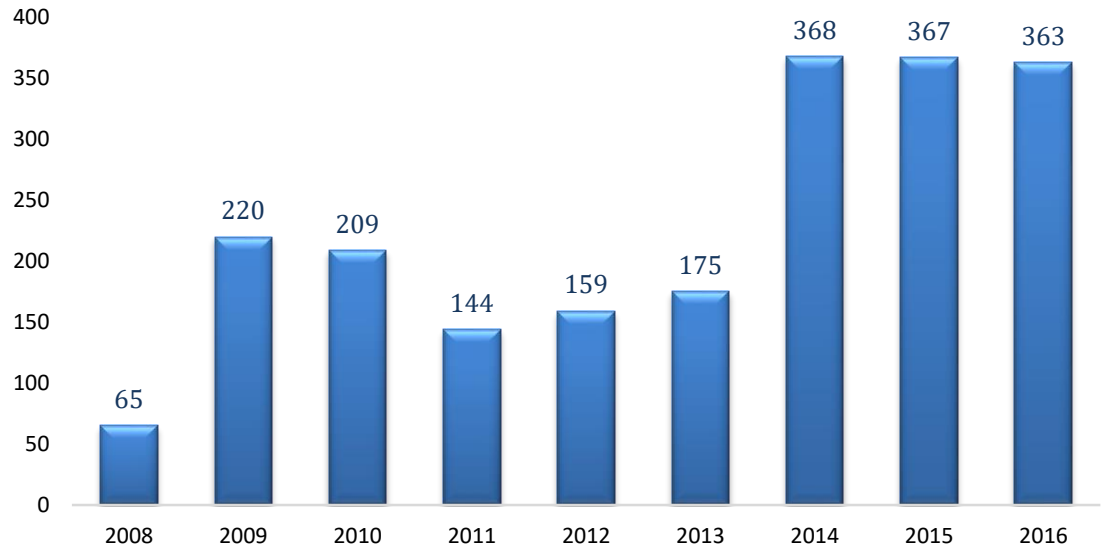
Na počátku kybernetického zločinu jsme se setkávali se schopností útočníků obelstít bezpečností mechanismy, nicméně jak se postupně kybernetické útoky začaly profesionalizovat, útočníci změnili taktiku – zůstat co nejdéle nenápadní. (Votruba, 2016) Běžní uživatelé v dnešní době až moc důvěřují informačním systémům, než by bylo vhodné a neuvědomují si otázku bezpečnosti. Proto si v této části práce vymezíme nelegální aktivity v kyberprostoru, jenž mohou ohrozit každého z nás.

3.5.1 Phishing

Phishing je nelegální aktivita, která spočívá v získání důvěrných informací nebo odhalení identifikačních komunikačních dat používaných při online službách. Obětí útoku mohou být uživatelé internetu, kterým může být vyprázdněn bankovní účet, či bankovní instituce, jenž mohou ztratit svou dobrou reputaci v očích klientů. Slovo phishing pochází z anglického spojení „*password harvesting fishing*" a znamená doslova sběr hesel rybařením. (Kostrecová et al., 2010)

Útok je obvykle proveden formou e-mailové zprávy s cizí identitou nebo autoritou s cílem zmanipulovat uživatele k získání osobní informace. V prvním případě je uživatel vyzván k navštívení stránky, která vypadá jako originální. Stránka je ale ve skutečnosti podvržena útočníkem. Ve většině případů musí uživatel vyplnit pole s uživatelským jménem a heslem či číslem kreditní karty, které útočníkovi poslouží k ovládnutí účtu či ukradení peněz. (Vacca, 2013) Další možností je využívání mobilního telefonu, kdy uživatel v domnění, že komunikuje se svou bankovní institucí, předává autentizačnímu formuláři své identifikační údaje. Tento útok využívá VoIP systémy (volání prostřednictvím internetu). (Kožíšek a Písecký, 2016)

Jak můžeme vyčíst z grafu bezpečnostního týmu pro koordinaci řešení bezpečnostních incidentů v počítačových sítích provozovaných v České republice CSIRT.CZ (2017b) počet případů phishingu je od roku 2015 na poklesu, což může být způsobeno právě zavedením nového zákonu tentýž roku.



Obr. 5 Vývoj počtu incidentů phishingu v ČR
Zdroj: CSIRT.CZ, 2017b

Žádný systém nám nemůže poskytnout stoprocentní ochranu před phishingem, nicméně riziko potencionálního boje s útokem můžeme snížit dodržováním určitých bezpečnostních zásad. První z nich se týká vlastnění kvalitního antivirového programu a firewallu. Vzhledem k tomu, že jsou útočníci velice nápaditi a inovativní, je

potřeba všechny programy pravidelně aktualizovat. Například již zmíněný antivirový program obsahuje databázi, ve které je popsána většina známých virů a pokud program neaktualizujeme, databáze se neobnoví a program tak nebude schopen bránit nás před novými viry. Při surfování na internetu bychom měli používat aktualizované prohlížeče, nejlépe ty, které už v sobě mají zahrnutou phishingovou ochranu. (Dočekal, 2008)

Nicméně ani sebelepší software nikomu nepomůže, pokud se nebude chovat alespoň trochu předvídavě. Nejčastějším trikem podvodníků, je snaha vyvolat pocit, že je třeba přihlásit se do svého internetového bankovnictví ihned, jinak se potenciální dluh zvýší či o své peníze přijdeme. Tyto finty je potřeba rozeznat už ze začátku. Převážně bychom neměli otevírat žádné odkazy z e-mailu a měli bychom se do svého bankovnictví přihlašovat pouze z oficiálních stránek banky. Musíme totiž myslet na to, že žádná instituce po nás nikdy nebude vyžadovat přihlašovací údaje e-mailem. Dalším způsobem, jak poznat že se jedná o phishingový email, je rozpoznání nespisovné, či celkově špatné češtiny. Pokud se ani přes tyto bezpečnostní opatření útoku neubráníme, je potřeba okamžitě informovat svou bankovní instituci a problém začít řešit.

3.5.2 Pharming

Na rozdíl od phishingu, který žádá od uživatele kliknutí na odkaz, pharming uživatele přímo připojí na falešnou webovou stránku, i přesto, že ji zadal správně. Je tudíž mnohem sofistikovanějším útokem, který staví na manipulaci s DNS záznamy (systém doménových jmen). Pojem pharming se do češtiny překládá jako hospodaření. Cílem útočníka je automatické přesměrování na falešné webové stránky imitující skutečnou stránku, aby získaly přístupové údaje uživatele. Pharmer změní v DNS přepojení mezi doménovým jménem a IP adresou stránky. Člověk se tedy stane obětí, i když zadal jméno domény správně. (Matyáš et al., 2008)

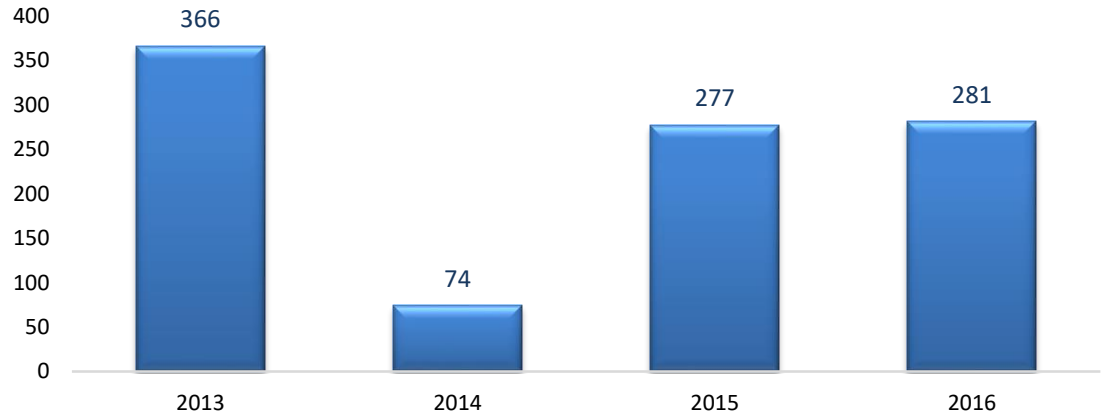
Podezřelé stránky můžeme rozeznat nestandardním chováním internetbankingu, například ve formě údajů, které po nás internetbanking běžně nepožaduje. Obecně můžeme říct, že obrana proti pharmingu není vůbec jednoduchá. Mezi kroky, které můžeme podniknout, patří využívání pravidelně aktualizovaného antivirového programu, správně nakonfigurovaného firewallu a využívání vhodných prohlížečů. Pro snížení rizika napadení uživatelů zavedly banky například autentizační a autorizační SMS kódy či elektronické klíče.

3.5.3 Skimming

Pojem skimming označuje typ podvodu, při kterém dochází k nezákonnému zkopírování informací obsažených na platební kartě a k následnému odcizení finanční hotovosti z účtu majitele karty. Skimmovací zařízení je zařízení provádějící neoprávněné kopírování dat. Se skimmingovým útokem se setkáme nejčastěji u platebních terminálů a bankomatů, kde útočník nainstaluje zařízení pro kopírování dat, uložených na magnetickém proužku platební karty k otvoru pro vložení platební karty na

bankomatu. Dále nainstaluje zařízení pro kopírování PIN kódu formou falešné klávesnice nebo kamery. Tyto dva kroky vyžadují fyzickou přítomnost útočníka. Po získání potřebných informací si útočník vytvoří duplikát platební karty a použije jej k neoprávněnému výběru finanční hotovosti z účtu majitele karty. Získané finanční prostředky následně zlegalizuje. (Policie ČR, ©2017)

V roce 2016 národní centrála proti organizovanému zločinu registrovala celkem 281 skimmingových útoků. Trestné činy byly páchány především na území hlavního města Prahy, v Libereckém kraji, Středočeském a Jihomoravském. Útoky se zabývaly především skupiny bulharských a rumunských občanů. (Policie ČR, ©2017) Podíváme-li se na následující graf, můžeme říct, že oproti roku 2015 můžeme v roce 2017 mluvit o mírném navýšení v počtu skimmingových útoků.



Obr. 6 Skimming v ČR
Zdroj: Policie ČR, ©2017

I přes velkou snahu bankovních institucí chránit bankomaty před skimmovacím zařízením se v ČR stále vyskytují případy tohoto podvodu. Při výběru peněz z bankomatu bychom si měli všímat nezvyklých a podezřelých věcí, jako je například přelepení klávesnice fólií. Poté by měla následovat kontrola, zda není v dohledu někdo, kdo by mohl lehce zpozorovat náš PIN, a při jeho následném zadávání bychom si měli zakrýt klávesnici druhou rukou. V případě podezření je vhodné uvědomit příslušný peněžní ústav či kontaktovat policii.

3.6 Pojištění internetového rizika

Ani na první pohled zdajícímu se zabezpečenému informačnímu systému nemůžeme zcela stoprocentně věřit. Proto je nutné se zamyslet nad tím, jak se krýt v případě vzniklé finanční ztráty. Pro případ, že se naskytne nepříjemná událost na internetu nebo s platební kartou, nabízí banky či pojišťovny produkt pojištění internetového rizika. Toto pojištění slouží pro případy zneužití vašich identifikačních či autorizačních údajů na internetu, zneužití platební karty a dalších nepříznivých událostí, jako je poškození pověsti na internetu. Pojistitel nabízí k pojištění asistenční

služby ve formě právní konzultace či IT asistence při problémech s výpočetní technikou. Pozor si musí dát pojištěnci na otázku územní platnosti, která se pro jednotlivé kategorie liší. Veškeré informace pojistných nebezpečích, výluk z pojištění a dalších smluvních podmínkách nalezneme ve všeobecných pojistných podmínkách konkrétního pojistitele. (Simoglu, 2016)

3.7 Kybernetické riziko v souvislosti s platebním stykem

Inovace v bankovnictví s sebou nemusí nést vždy pozitivní fungování. Potvrzuje to i fakt, že v závislosti na rychle vyvíjející se nové bankovní produkty či služby, rostou také počty negativních inovací ve formě bankovních podvodů. (Zeman, 2015) I přestože dle studie společnosti Grant Thornton Advisory jsou české banky v rámci zabezpečení elektronických plateb na nadstandartní úrovni, musí brát občané na vědomí lidský faktor, jenž je stále považován za největší příčinu vnějšího narušení bezpečnosti. (Šimůnková, 2016) Riziko kybernetického útoku značně zvyšuje nedostatečná informovanost a neznalost tématu bezpečnosti platebních prostředků uživatelů internetu a právě toho útočníci využívají.

Nejrozšířenějším útokem na finanční prostředky byl v roce 2016 finanční podvod – phishing, kde se útočníci snažili získat peníze od uživatelů vydáváním se za bankovní instituci. Každý čtvrtý útok využil falešné bankovní informace – oproti roku 2015 se jedná o nárůst o 8,31 procentního bodu. Uvedla to antivirová společnost Kaspersky Lab (2017) ve své zprávě za rok 2016.

Důkazem, že existence kybernetických hrozeb je stále aktuálnější, jsou pravidelné aktuality od českých bank o možném útoku. Při ohlédnutí za prvním čtvrtletím roku 2017, můžeme narazit hned na několik případů kybernetických útoků. Například Česká spořitelna opět v únoru 2017 zaznamenala novou podobu podvodného emailu, jenž se snažil vylákat od uživatelů přihlašovací údaje. I přestože měl email viditelné prvky klamného emailu (chybná emailová adresa či slova bez diakritiky), pár jedinců na odkaz v emailu kliklo. (Česká spořitelna, 2017b) Terčem útoků je v roce 2017 také ČSOB, která už stihla varovat klienty přes falešnými exekučními emaily, podvodnou mobilní aplikací společnosti DHL, s cílem infikování softwaru malwarem a získání tak přístupových kódu do bankovnictví, i instalací aplikace, jenž vyvolává dojem, že se jedná o software mobilního bankovnictví ČSOB Smartbanking. (ČSOB, 2017) Nicméně nejenom klienti bank se mohou stát terčem platebních útoků. Začátkem roku 2017 útočníci zacílili i na zákazníky České pošty, jenž byli vyzváni pomocí SMS k instalaci aplikace. Součástí odkazu k jejímu stažení byl ovšem vir, který měl útočit na elektronické bankovnictví vlastníků mobilního telefonu. (Česká pošta, 2017) Vlna podvodných SMS se nevyhnula ani největšímu prodejci elektroniky – společnosti Alza.cz. SMS byla mířena na náhodná čísla a slibovala 500 Kč na nákup, pokud bude objednávka provedena přes jejich aplikaci. Samozřejmě instalací aplikace mohli spotřebitelé přijít o zneužití osobních údajů. (Alza.cz, 2017)

Žijeme v době, kdy je stále rychlejší nástup nových hrozeb, větší komplexnost systémů i rizik a vyšší požadavky na bezpečnost. Z kvantitativního pohledu národní CSIRT vyřešila v roce 2016 přes 1000 incidentů, což není zrovna málo. (Duračinská,

2017) Řešením kybernetické kriminality není represe, ale prevence a zvýšená opatrnost uživatelů. Toto téma bychom proto neměli brát na lehkou váhu a zvážit čas i peníze investované do větší bezpečnosti.

3.8 Akademické práce na téma kybernetické bezpečnosti

V této kapitole se zaměříme na analýzu prací, které se zabývaly podobným tématem a jež nám mohou, byť malým způsobem, přispět. Pro vyhledání jsme využili serveru theses.cz, který slouží jako národní registr závěrečných prací. V úvahu byly brány pouze ty práce, týkající se období posledních 3 let. Takto krátké období jsme uvažovali z důvodu aktuálnosti tématu a rychle měnícímu se vývoji. Použitá klíčová slova byla následující: kybernetické riziko, internetová kriminalita a platební prostředek.

První práce, jež stojí za zmínku, se zabývá analýzou využívání elektronických platebních prostředků a systémů. Její autor, Čech (2014), vyhodnocuje vlastní dotazníkové šetření a provádí komparaci s daty nashromážděnými v rámci zpracování jeho bakalářské práce před 4 lety. Výsledky porovnává i s dalšími, sekundárními daty, jež mu poskytlo sdružení APEK. Práce se zaměřuje především na formu a frekvenci plateb, zatímco my se pro účely naší bakalářské práce v dotazníkovém šetření zaměříme konkrétně na bezpečnostní kroky veřejnosti, podnikající v rámci jejich ochrany peněz.

Jahodář (2016) ve své bakalářské práci předává informace o problematice kybernetického rizika se zaměřením právě na platební styk. Práce má vytyčené 3 cíle, z nichž prvním z nich je identifikace rizik platebního styku. Druhý cíl si stanovil autor jako popsání kroků, jenž vedou ke zvýšení kybernetické bezpečnosti a třetí, vyhodnocení dotazníkového šetření zaměřeného na informovanost veřejnosti o dané problematice. Co však práce neobsahuje, je rozbor bezpečnostních prvků a opatření, na které by se měl uživatel zaměřit při používání konkrétních platebních prostředků. Právě této části bude věnována největší pozornost v rámci naší bakalářské práce.

V práci s názvem Problematika sociálního inženýrství v souvislosti s elektronickými platebními systémy, si kladla autorka Chrástová (2015) za cíl snížit u studentů Mendelovy univerzity míru rizika zneužití citlivých údajů v oblasti platebního styku. Toho chtěla bakalantka docílit vyhodnocením dotazníku s primárními daty, převážně zaměřeného na znalost studentů v dané problematice, a stanovit z něj soubor opatření, jenž by tato rizika měl minimalizovat. Naše bakalářská práce se orientuje převážně na stupeň realizace bezpečnostních opatření na platebních prostředcích, sloužících k ochraně před kybernetickými útoky, než na vzdělanost respondentů v dané problematice, jako u bakalantky Chrástové.

V rámci shrnutí bychom mohli říct, že žádná z prací neobsahovala podrobný výzkum bezpečnostních prvků a opatření, které uživatelé při manipulaci se svými penězi v rámci elektronického a bezhotovostního bankovnictví využívají. Poukazovanou mezeru bychom chtěli zaplnit vypracováním této bakalářské práce a výše zmíněné práce využít jako inspiraci pro náš průzkum.

4 Metodika

Pro dosažení hlavního cíle zvolíme empirickou metodu dotazníkového průzkumu, jehož rozbor je předmětem vlastní části bakalářské práce. Při tvorbě dotazníkového šetření použijeme metodiku EUROSTATU, jenž každoročně shromažďuje data o míře využívání informačních technologií (ICT) domácnostmi a jednotlivci EU. Velká část nashromážděných údajů je používána v rámci jednotného digitálního trhu, který otevírá digitální příležitosti pro lidi a podniky, a má za cíl posílit postavení Evropy v oblasti digitálního hospodářství. (EUROSTAT, 2016) Nicméně výzkum EUROSTATU z mého pohledu postrádá hlubší zaměření se na bezpečnost ICT, konkrétně bezpečnost elektronického a bezhotovostního platebního styku, na které je zaměřena právě tato bakalářská práce. Totéž můžeme říct i o Českém statistickém úřadu, jehož dotazníky v oblasti ICT odpovídají struktuře modelového dotazníku EUROSTATU, a také nezahrnují výše zmíněné zaměření se na bezpečnost ICT. Veškeré zkoumané oblasti v dotazníku byly podrobně definované v rešeršní části bakalářské práce a sloužily jako podklad k realizaci dotazníkového šetření.

Samotná tvorba dotazníku se řídí Metodickým manuálem pro tvorbu statistik informační společnosti na rok 2016, na základě kterého si definujeme:

Cílovou skupinu – EUROSTAT zkoumá tři cílové skupiny – jednotlivce, domácnosti a podniky, z nichž se v bakalářské práci zaměříme pouze na jednotlivce. Cílovou skupinu tvoří všechny fyzické osoby ve věku 16 až 74 let rozdělených do 6 skupin dle věku 16–24, 25–34, 35–44, 45–54, 55–64, 65–74 let. Musíme brát v úvahu fakt, že populace jednotlivců ve věku 16 až 74 let, představuje dle ČSÚ (2016) v ČR přibližně 76,7 % z celkového počtu obyvatel, tudíž výsledky nebudou reprezentativní pro celkovou populaci, ale pouze pro tuto podskupinu.

Typy jevů a pozorované proměnné – ve výzkumu použijeme kvantitativní proměnné s cílem shromáždění informací o frekvenci využívání, ale také kvalitativní proměnné k získání nenumerických či kategorických dat. Budeme především využívat spojité kvantitativní proměnné, tedy odpovědi v určitém rozsahu. V dotazníku se objeví i binární otázka s výběrem odpovědi ano či ne. Otázky budou otevřeného, uzavřeného i polouzavřeného charakteru. V rámci uzavřených otázek se budou vyskytovat trichotomické otázky, alternativní a výčtové.

Období šetření – podle přílohy II nařízení Komise (ES) č. 859/2013 ze dne 5. září Evropského parlamentu a Rady o statistikách Společenství o informační společnosti by mělo být období šetření pro statistiku stanoveno na první čtvrtletí roku. Od prvního čtvrtletí se odvíjí také otázky na frekvenci v rámci dotazníkového šetření, v nichž se ptáme přibližně na předcházející 3 měsíce (referenční období), což omezí sezónní zaujatost.

Sociodemografické údaje – pro potřeby bakalářské práce zkoumáme věk v rámci věkových skupin, pohlaví respondentů a vzdělání rozčleněné na základní, vyučen/a v oboru, středoškolské s maturitou a vysokoškolské. Zaměstnanost a geografické údaje nebudou zkoumané.

Způsob sběru dat – nejčastějšími metodami využívanými EUROSTATEM jsou rozhovor tváří v tvář či telefonní rozhovor, v menší míře se využívají průzkumy zasílané poštou či internetové výzkumy. I přesto si mohou jednotlivé země zvolit vlastní metodu získání dat, popřípadě metody kombinovat. Pro účely této bakalářské práce využijeme elektronického dotazníku, sdíleného na internetu. Cílem našeho sběru dat je získat 400 respondentů různých věkových skupin. Poměr mužů a žen se bude řídit ČSÚ (2016), který udává, že je v ČR 51 % žen a 49 % mužů. Stejný poměr tedy použijeme v dotazníkovém šetření.
Výsledky – vyhodnocené anonymní odpovědi následně interpretujeme, podobně jako EUROSTAT ve svých výzkumech, slovním vyjádřením a doplníme grafickou metodou, kde využijeme koláčové a sloupcové grafy. Výsledky budou srovnávány převážně v rámci pohlaví, jež rozdělíme rovnoměrně dle poměru mužů a žen v České republice. Setkáme se také s komparací v rámci dosaženého stupně vzdělání. Ve výzkumu se vyskytne hodně otázek, na které sice neexistuje objektivně správná odpověď, ale některá z variant či jejich kombinace je považována za zodpovědnější. U těchto otázek navrhneme nejvhodnější možné řešení a budeme polemizovat s odpověďmi respondentů. Dotazník bude také zahrnovat otevřenou otázku, jež se táže na osobní zkušenosti uživatelů s kybernetickou kriminalitou. Jednotlivé případy slovně ohodnotíme a pokusíme se jednotlivcům udělit obecná doporučení k zamezení dalšího napadnutí. V návaznosti na sekci zabývající se kybernetickým rizikem vytvoříme doporučení pro zlepšení informovanosti uživatelů o bezpečnostních rizicích. Ke komplexním výsledkům šetření dále zaujmeme stanovisko a v šesté kapitole provedeme komparaci s výsledky jiných výzkumů. (Eurostat, 2016)

5 Vlastní práce

Abychom mohli zhodnotit informovanost veřejnosti o jejich rizicích v dané problematice a zjistit využívání bezpečnostních prvků a opatření, využili jsme již zmíněnou metodu empirického výzkumu – dotazníkové šetření. Rozboru a vyhodnocení výsledků výzkumu je věnována právě tato část bakalářské práce.

Dotazník byl sestaven dle vlastního uvážení, na základě získaných teoretických znalostí k tématu, a také aby odpovídal cíli bakalářské práce. Pro lepší přehlednost jsme jej rozdělili do 8 sekcí, přičemž každá sekce se týkala specifické oblasti a pomáhala k splnění těchto účelů šetření:

- zjištění využívání nástrojů elektronického a bezhotovostního platebního styku včetně frekvence placení,
- ověření využívání bezpečnostních opatření a prvků jednotlivých nástrojů,
- znalost respondentů oblasti kybernetické bezpečnosti.

První sekce byla věnována oblasti platebních karet. Cílem bylo zjištění, jak často respondenti platbu kartou na internetu využívají, a zda vůbec. Při volbě možností odpovědí jsme se inspirovali metodikou ČSÚ, jež se ve svých dotaznících táže na období posledních 3 měsíců (stejně jako EUROSTAT) a dělí frekvenci na 1 – 2x, 3 – 5x, 6 – 10x, více než 10x za měsíc a nikdy. My jsme možnost *„nikdy“* dále konkretizovali, a respondenti si tak museli vybrat, z jakého důvodu tuto službu nevyužívají. Ti, jenž platbu kartou využili alespoň jednou za poslední 3 měsíce, byli dále odkázáni na otázku bezpečnostních prvků a opatření, které využívají pro snížení rizika možného útoku. Tato otázka vycházela z rešeršní části práce, kde byly veškeré zmíněné prvky a opatření v rámci platební karty na internetu blíže specifikovány.

Na podobné bázi byla stavěna i další sekce, jež se týkala platby mobilním telefonem s technologií NFC. Stejně jako u prvního oddílu, účastníci výzkumu odpovídali na otázku týkající se frekvence placení pomocí toho platebního prostředku. Následně, podle možnosti odpovědi, byli odkázáni na další otázku. Pro ty, jenž zvolili využívání této možnosti platby, byla připravena otázka na využívaná bezpečnostní opatření. Zbytek respondentů byl odkázán na otázku týkající se bezkontaktní platby.

V rámci další sekce jsme se snažili o získání informací o využívání prostředků bezkontaktní platby. Respondenti měli možnost výběru více odpovědí, jež byly v rámci literární rešerše blíže popsány. Cílem bylo zjištění, zda jsou dotazovaní spíše konzervativní či dychtiví po inovacích v oblasti platebních technologií. Opět zde byly možnosti i pro ty, kteří službu bezkontaktní platby nevyužívají s nutností odpovědi z jakého důvodu.

Jestliže mluvíme o elektronickém platebním styku, je nutné zmínit i oblast internetového bankovnictví, které byla věnována další sekce. Mimo otázky na frekvenci a bezpečnostní opatření uživatelů jsme se respondentů ptali na formu autorizace bankovních operací.

Mezi další inovativní platební možnost řadíme mobilní bankovnictví. I jemu byla věnována jedna z dalších sekcí. Stejně jako u internetbankingu jsme zjišťovali

četnost platby v rámci posledních 3 měsíců a využívání bezpečnostních prvků a opatření, jenž byly definované v rešeršní části.

Elektronickým peněženkám, jakožto dalším platebním prostředkům, se také věnovala jedna ze sekcí. V rámci otázek jsme se ptali dichotomickou otázkou na využívání elektronických peněženek. Účastníci výzkumu, jenž tuto formu platby využívají, byli následně odkázaní na otázku bezpečnostních opatření.

Další sekce se soustředila na zmapování faktického stavu znalosti respondentů v oblasti kybernetické bezpečnosti. V prvních otázkách jsme zjišťovali, jak moc respondenti dbají na svou ochranu, když jde o elektronickou poštu, a jak by se zachovali, pokud by jim takový email do schránky přišel. V návaznosti na internetovou kriminalitu se v dotazníku vyskytla i otázka na pojištění internetových rizik. Součástí sekce byla i otevřená otázka na osobní zkušenosti s internetovou kriminalitou, jež byla na dobrovolné bázi. Poslední otázka této sekce byla formou kvízu a ověřovala znalost konkrétních pojmů kybernetických útoků. Volba jednotlivých útoků, stejně jako přiřazené definice, vycházela z literární rešerše.

Poslední sekce byla věnována základním ukazatelům popisujícím cílovou skupinu – sociodemografickým údajům. Jak již bylo v metodické části práce zmíněno, zkoumali jsme pohlaví, věk a vzdělání respondentů.

Před zahájením výzkumu byl realizován předvýzkum na vzorku 10 respondentů, jehož cílem bylo zkorigovat nesrozumitelně položené otázky, otestovat jednoznačnost otázek a upravit dotazník do koncové podoby. Poté byl proveden samotný výzkum na základě optimálního dotazníku, vytvořeného pomocí anonymního Google formuláře v elektronické formě. Důvodem výběru této formy sběru dat byly podstatné faktory – rychlost šíření, eliminace finančních nákladů a možnost exportu dat do různých formátů. Při vyplňování online dotazníku byl kladen důraz na zachování standardu péče o ochraně osobních údajů a zajištěna anonymita pro účely vědecké činnosti. Distribuce probíhala převážně formou internetového šíření na sociálních sítích, kde se dostala k mladším generacím, jež tvoří velkou skupinu respondentů našeho dotazníkového šetření. Dalšími místy zveřejnění byly diskuzní fóra, webové stránky seniorů, z důvodu zastoupení starších věkových skupin, a další tematické stránky, pro zastoupení jedinců, jenž sociální sítě nevyužívají.

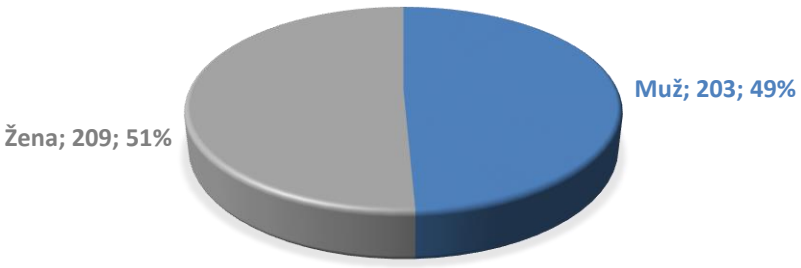
S ohledem na nařízení Komise jsme splnili i předpoklad referenčního období, jenž mělo být v prvním čtvrtletí sledovaného roku. Dotazníkové šetření na základě doporučení proběhlo od 22. 2. 2017 do 4. 4. 2017.

Otázky ve vlastní části práce nebudou členěny podle pořadí, ve kterém se vyskytovaly v dotazníku, nýbrž podle logické návaznosti a jednotlivých okruhů. Znění dotazníku je možné nalézt v příloze této bakalářské práce.

5.1 Struktura výběrového souboru

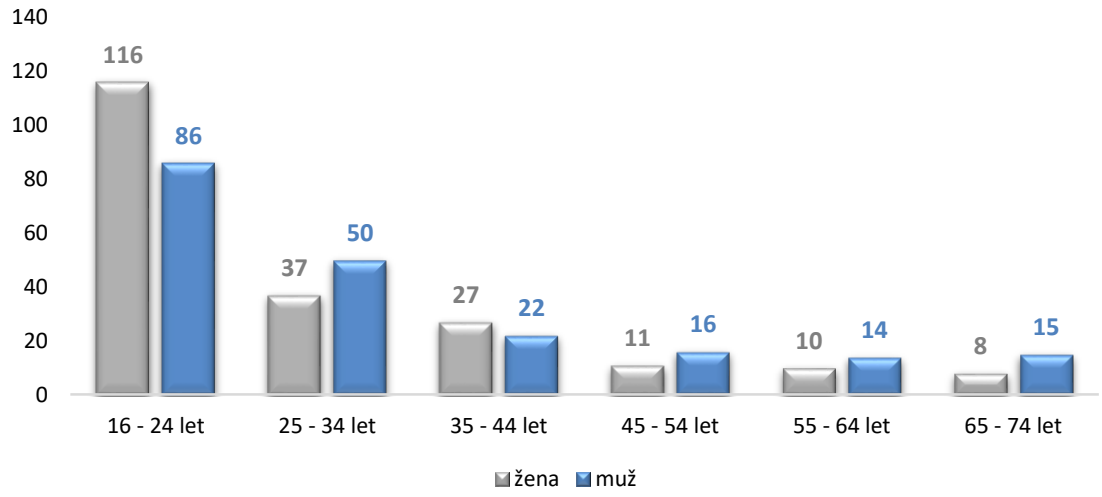
I přesto, že byly klasifikační otázky na pohlaví, věk a nejvyšší dosažené vzdělání respondentů umístěny na konec dotazníku, budeme se jimi zabývat hned na úvod. Co se rozsahu výběrového souboru týče, šetření bylo provedeno na 419 respondentech. Nicméně, jak je již v metodice uvedeno, složení výběrového souboru šetření by

v této práci mělo odpovídat doporučení Eurostatu. Z toho důvodu jsme vyloučili odpovědi věkové skupiny pod 16 let a nad 74 let. Po vyřazení odpovědí těchto respondentů se dostáváme na 412 adekvátních odpovědí. Dalším požadavkem, vymezeným v metodice, je poměrové složení mužů a žen zastoupených v dotazníkovém šetření. Vzhledem k tomu, že nám odpovědělo 203 mužů a 209 žen, jak můžeme vidět i na Obr. 7, tento předpoklad splňujeme.



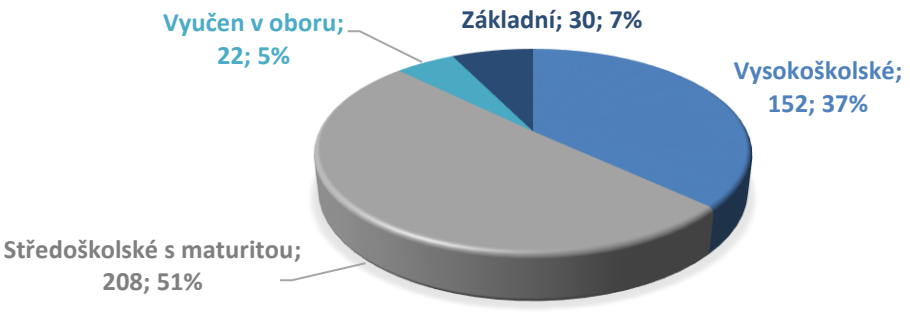
Obr. 7 Pohlaví respondentů (Otázka č. 21)

V dotazníkovém šetření jsme se snažili i o vyvážený poměr mužů a žen v jednotlivých věkových kategoriích, nicméně vzhledem k tomu, že se jednalo o anonymní průzkum, jenž byl převážně šířený elektronicky, nemohli jsme tento vztah výrazně ovlivnit. Markantní rozdíl v poměru pohlaví respondentů můžeme vidět u první a druhé věkové kategorie. Z Obr. 8 můžeme vyčíst, že nejpočetnější věkovou skupinou jsou v našem případě respondenti ve věku 16–24 let, což je zapříčiněno převážně způsobem šíření a faktem, že internet využívají z velké části mladí lidé. (ČSÚ, 2016)



Obr. 8 Věkové kategorie respondentů (Otázka č. 22)

Abychom mohli vyhodnotit, jestli má využívání moderních platebních metod a jejich bezpečnostních opatření vliv na dosažený stupeň vzdělání respondentů, bylo nutné respondenty členit také podle vzdělání. Nejčetnější skupinou našeho šetření jsou respondenti se středoškolským vzděláním zakončeným maturitou, jenž mají v šetření 51% zastoupení. Na druhou stranu nejméně je respondentů se základním vzděláním, což je převážně způsobeno vyloučením věkové skupiny pod 16 let.



Obr. 9 Dosažené vzdělání respondentů (Otázka č. 23)

Vzhledem k tomu, že se většina otázek týkala platebních prostředků, k nímž musíte mít zřízený běžný účet, byla úvodní otázka zaměřena právě na něj. Posloužila nám jako filtrace za účelem vyčlenění z první části výzkumu těch respondentů, jenž účet zřízený nemají. Tito respondenti byli přesměrováni až na otázky, na které mohli odpovídat, aniž by účet museli mít, a nebyli tak z výzkumu zcela eliminováni. Vycházejíce z Tab. 2 můžeme říct, že se jedná právě o 2,4 % respondentů, jenž nevyužívají možnost běžného účtu. Jedná se převážně o respondenty ve věku 65 – 74 let, kteří pravděpodobně odmítají bankovní účet z důvodu nepřehledné administrativy, které nerozumí. Běžný účet nemají také ti, kteří jej de facto k ničemu nepotřebují. V dalších kapitolách budeme tedy uvažovat o výběrovém souboru o 402 respondentech.

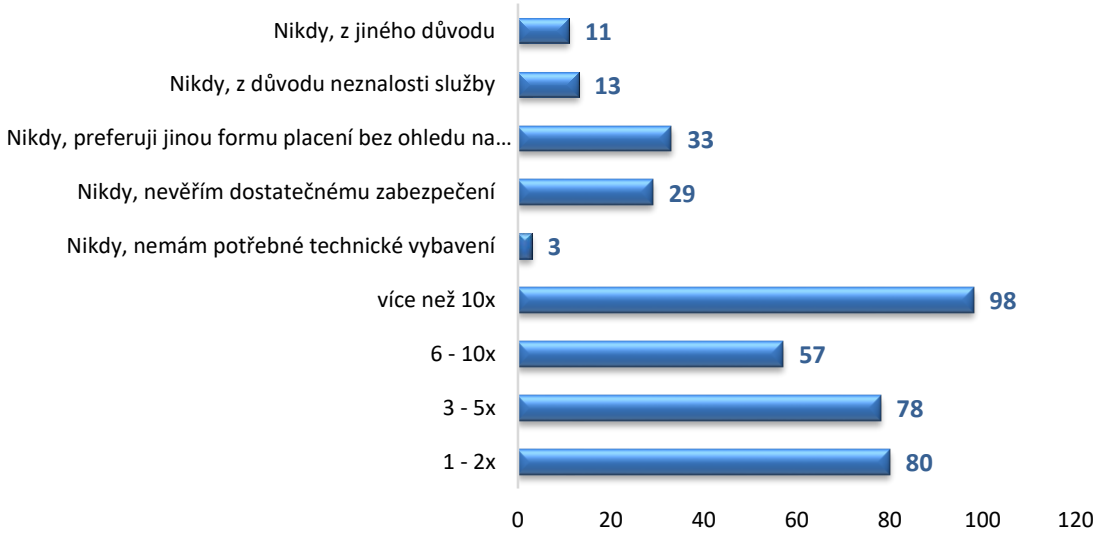
Tab. 2 Zřízení běžného účtu (Otázka č. 1 – Máte zřízený běžný účet?)

	Absolutní četnost	Relativní četnost
Ano	402	97,6 %
Ne	10	2,4 %

5.2 Platba kartou na internetu

Způsobů jak zaplatit za zboží či služby je víc než dost a už je jenom na obchodníkovi, kterou platební metodu bude na svých stránkách nabízet. Avšak k vybudování silného postavení mezi konkurencí je potřeba nabídku platebních metod nepodceňovat, protože právě malý výběr může být důsledkem nedokončení nákupu. Dle pro-

vedeného dotazníkového šetření můžeme říct, že z celkového počtu 402 respondentů, jenž mají u své banky zřízený účet, využívá platbu kartou na internetu celých 77,9 %. Největší přínos a důvod vysokého procenta respondentů můžeme spatřovat převážně v rychlosti provedení platby a faktu, že jsou mezi námi i obchodníci, jenž jiný způsob platby neumožňují. Nicméně za relativně vysokým podílem mohou stát i poplatky související s ostatními způsoby úhrady za zboží či služby objednané právě z internetu. Na druhou stranu pro mnoho klientů jsou jiné formy placení stále určitou formou jistoty, že za své peníze skutečně něco obdrží (např. platba dobírkou). Toto tvrzení dokazuje i Obr. 10, kde můžeme vidět, že 33 respondentů preferuje jinou formu placení, bez toho aniž by se ohlíželo na zabezpečení platby kartou na internetu. Z Obr. 10 taktéž můžeme vyčíst, že se stále našlo 29 respondentů, konkrétně 14 žen a 15 mužů, jenž neplatí na internetu kartou právě z důvodu nedůvěry v dostatečné zabezpečení. Jedná se převážně o jedince se základním vzděláním, kteří jsou nejčetnější skupinou i v případě odpovědi *„nikdy, z důvodu neznalosti služby“*.

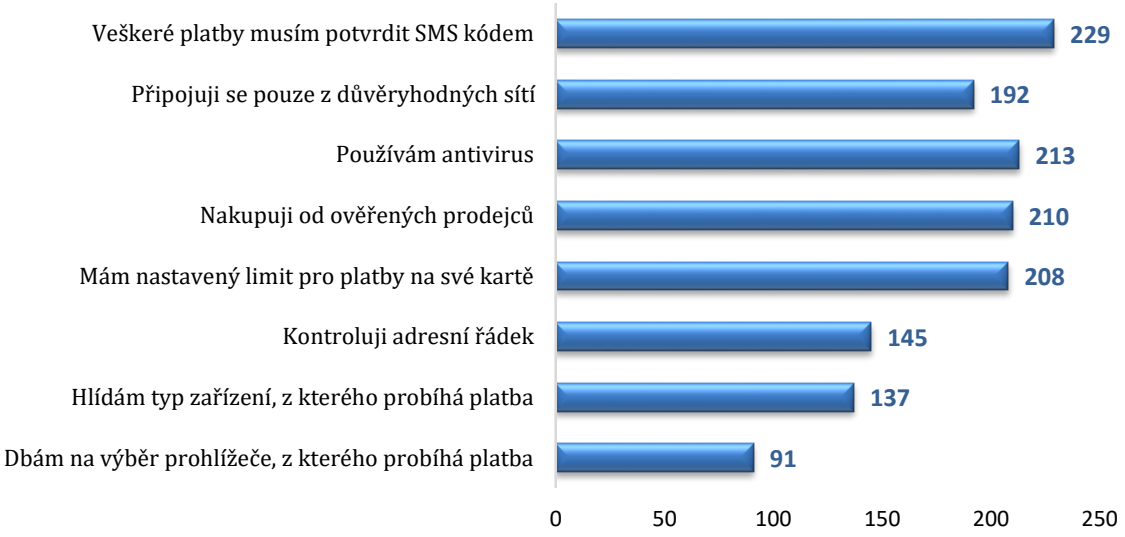


Obr. 10 Frekvence plateb na internetu (Otázka č. 2 – Kolikrát jste platil/a za poslední 3 měsíce platební kartou na internetu?)

Otázka na využívání bezpečnostních prvků při platbě kartou na internetu se týkala respondentů, jenž v předchozí otázce na frekvenci plateb na internetu (viz Obr. 10) odpověděli, že minimálně jednou za 3 předcházející měsíce tuto formu úhrady využili. Také je nutno podotknout, že tato otázka nemá správnou odpověď. Jednotlivé banky vydávají pouze bezpečnostní zásady, kterých by se klienti měli držet a poté už je na nich, jak s bezpečností jejich peněz naloží. Avšak platí pravidlo, že čím více bezpečnostních prvků budeme využívat, tím více zamezíme neoprávněnému přístupu. Právě z tohoto důvodu byla otázka zvolena jako výčtová a umožnila tak respondentům kombinovat několik možností odpovědí.

Ještě než se rozhodneme, že na internetu nakoupíme, měli bychom se ohlédnout na již zmíněné bezpečnostní opatření. Mezi první řadíme ověření prodejce. Pokud nemáme s vybraným obchodem zkušenosti, měli bychom si přinejmenším přečíst recenze a prověřit certifikaci či akreditaci obchodu. I přes velké riziko neobdržení zboží, neuskutečnění služby či zneužití údajů se stále našlo 33 % respondentů, jenž nedbají na výběr seriózního prodejce.

Nejčetněji využívaným bezpečnostním prvkem, který uvedlo 229 respondentů z 313, je využívání SMS kódu k potvrzení veškerých plateb. U zbylých 27 % respondentů můžeme předpokládat, že autorizování plateb nastavené vůbec nemají. Nicméně doufáme, že se s postupným rozšiřováním služby 3D Secure, jenž vyžaduje tuto formu autorizace vždy, bude riziko snižovat. Taktéž bychom chtěli zmínit nejvíce opomíjený element – volbu prohlížeče, na který dbá podle Obr. 11 pouze 91 dotázaných.



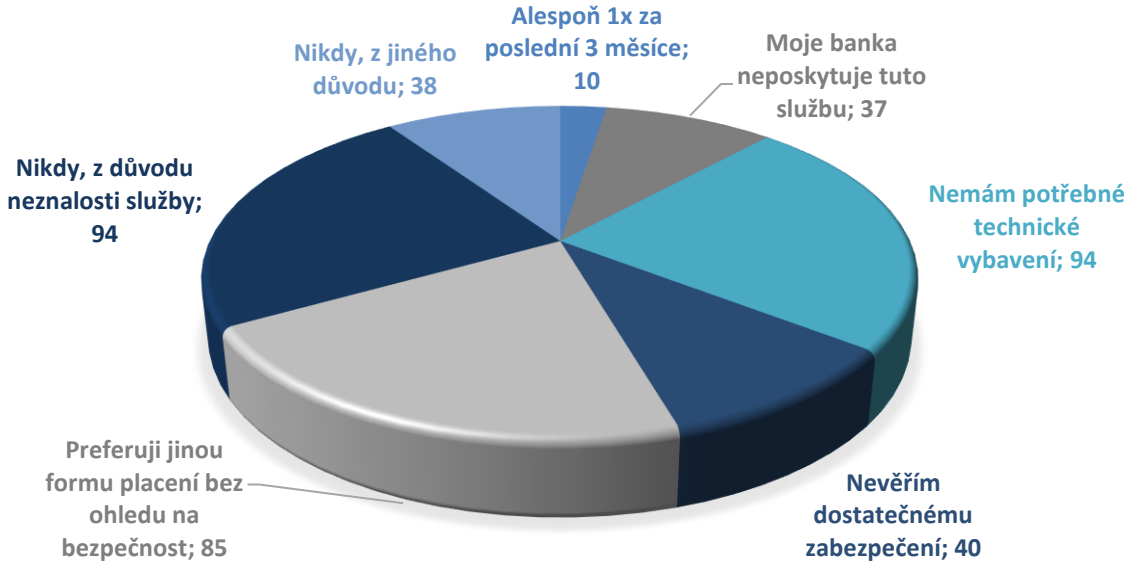
Obr. 11 Bezpečnostní prvky a opatření využívané při platbě kartou na internetu (Otázka č. 3 – Pokud platíte platební kartou na internetu, co děláte pro svou ochranu?)

5.3 Platba mobilním telefonem s technologií NFC

Překvapivé výsledky přinesla otázka na využívání platby mobilním telefonem s technologií NFC, kde pouze 14 respondentů uvedlo, že alespoň 1x za poslední 3 měsíce využilo tuto možnost úhrady za zboží či služby. Největší podíl má mužské pohlaví ve věku 16–24 let. Zbytek respondentů, který dělá 96 %, tuto možnost platby nikdy nevyužilo. Mezi dva základní uváděné důvody patří neznalost služby, jenž podle Obr. 12 uvedlo 94 tázaných, a nevlastnění potřebného technického vybavení. V obou dvou případech se ve větší části jedná o ženy. Dále můžeme říct, že celých 21 % zaujímá podíl lidí, kteří preferují jinou formu placení.

Nejčastěji uváděným bezpečnostním prvkem při platbě mobilním telefonem s technologií NFC je dle provedeného šetření omezení ve formě denního limitu pro

platby, jenž uvedlo 7 lidí ze 14. Nečekaným zjištěním je fakt, že 4 respondenti nevyužívají žádný bezpečnostní prvek v rámci ochrany jejich peněz při platbě mobilním telefonem. Jedná se převážně o respondenty ve věku 16–24 let. Méně častým uváděným opatřením je využívání PIN kódu pro potvrzení platby, využívaným pouze 4 respondenty.



Obr. 12 Frekvence plateb mobilním telefonem s NFC (Otázka č. 4 – Kolikrát jste za poslední 3 měsíce využil/a bezkontaktní platbu mobilním telefonem s technologií NFC?)

5.4 Bezkontaktní platební prostředky

Fakt, že je platební karta nejpoužívanějším platebním nástrojem dokazuje Tab. 3, jenž říká, že právě 85 % dotázaných tento instrument využívá nejčastěji. Ne moc známou alternativou k platební kartě, nicméně přesto využívanou 21 respondenty našeho dotazníkového šetření, je bezkontaktní platební nálepka. Výhodu této formy placení mohou lidé vidět ve formě snadného umístění kamkoliv a ve velikosti formátu. Když se podíváme na výsledky tzv. wearables (nositelného zařízení), není překvapivým zjištěním, že bezkontaktní platební náramek nikdo z dotázaných nevyužívá. Náramky nejsou v České republice totiž momentálně k dostání. Na druhou stranu u známějšího zařízení, bezkontaktních platebních hodinek, lze pozorovat, že se pomalu dostávají i na český trh. I přesto, že tuto formu úhrady zvolili pouze 4 účastníci výzkumu ve věku 16–24 let, dokazuje, že se tento druh platby pomalu dostává do povědomí spotřebitelů. Malý podíl respondentů může být převážně z důvodu vynaložení velké částky k získání těchto chytrých hodinek.

Podle odpovědí je zřejmé, že mezi lidmi stále převažuje kladné hodnocení bezkontaktních platebních nástrojů nad obavami ze zneužití. Nicméně je tu stále ta část respondentů, jenž bezkontaktní platební instrumenty nevyužívá. Možnost zaplatit za malý nákup do 500 Kč bez nutnosti zadání PIN kódu může být jedním z důvodu, proč mnoho lidí odrazuje od jejich použití. Přesvědčuje nás o tom i Tab. 3, kde je

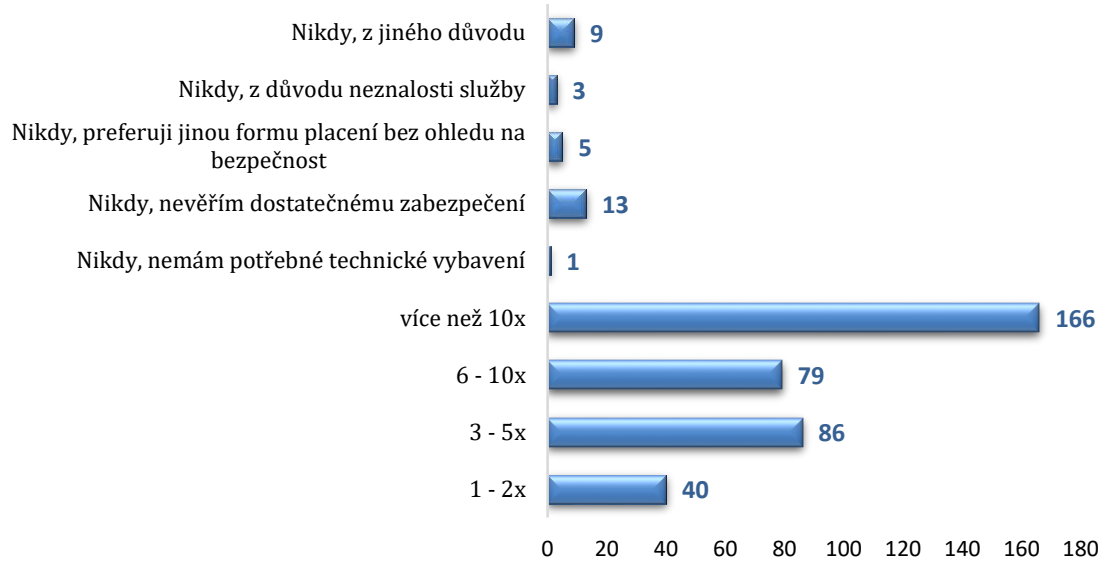
nejčastěji uváděným důvodem, proč respondenti neplatí bezkontaktně, nedůvěra v dostatečné zabezpečení, který uvedlo právě 7 % dotázaných. Nejčetnější skupinou byli respondenti ve věku 55–64 let. Lidé, jenž bezkontaktní platby nevyužívají, mohou využívat při platbě buď kontaktní platební kartu, nebo pro výběr hotovosti z účtu chodit přímo na pobočku banky.

Tab. 3 Bezkontaktní platby (Otázka č. 6 – Jakou formu bezkontaktní platby využíváte?)

	Muž	**Žena**	**Celkem**
Bezkontaktní platební KARTA	169	170	339
Bezkontaktní platební HODINKY	3	1	4
Bezkontaktní platební NÁLEPKA	12	9	21
Bezkontaktní platební NÁRAMEK	0	0	0
Mobilní telefon s technologií NFC	10	4	14
Žádnou, moje banka neposkytuje tuto službu	2	1	3
Žádnou, nemám potřebné technické vybavení	1	3	4
Žádnou, nevěřím dostatečnému zabezpečení	13	15	28
Žádnou, preferuji jinou formu placení bez ohledu na bezpečnost	6	8	14
Žádnou, z důvodu neznalosti služeb	2	0	2

5.5 Internetové bankovnictví

Ztracenému času ve frontách čekáním na vyřízení platebního požadavku odzvonilo s příchodem internetového bankovnictví. Pro většinu informačně gramotných jedinců je internetové bankovnictví součástí běžného života. Dokazuje to i Obr. 13, kde můžeme vidět, že právě 93 % dotázaných tuto službu hojně využívá. Z toho 166 respondentů, ve větší části mužů, bankovnictví využilo více než 10x za poslední 3 měsíce. 13 jedinců, jenž uvádí, že nedůvěřuje dostatečnému zabezpečení, si pravděpodobně neuvědomuje, že největším rizikem jsou v internetovém bankovnictví oni sami. Jedná se převážně o jedince ve věku 55–64 let. Při možnosti odpovědi *„nikdy, nemám potřebné technické vybavení“* musíme myslet na částečné zkreslení výsledků způsobem šíření dotazníku. Vzhledem k tomu, že byl dotazník šířen elektronicky, dostal se tak převážně k lidem, kteří mají potřebné technické vybavení k využívání služby internetového bankovnictví. 1 respondent, který tuto možnost zvolil, mohl dotazník vyplňovat z veřejně přístupného místa, kde ovšem nemusí natolik důvěřovat vybavení, že by se z něj přihlašoval do internetového bankovnictví. Je nutné taky poukázat na fakt, že všichni jedinci, kteří možnost internetového bankovnictví nevyužívají a přesto vlastní bankovní účet, musí pro učinění platebních příkazů docházet přímo na pobočku banky.

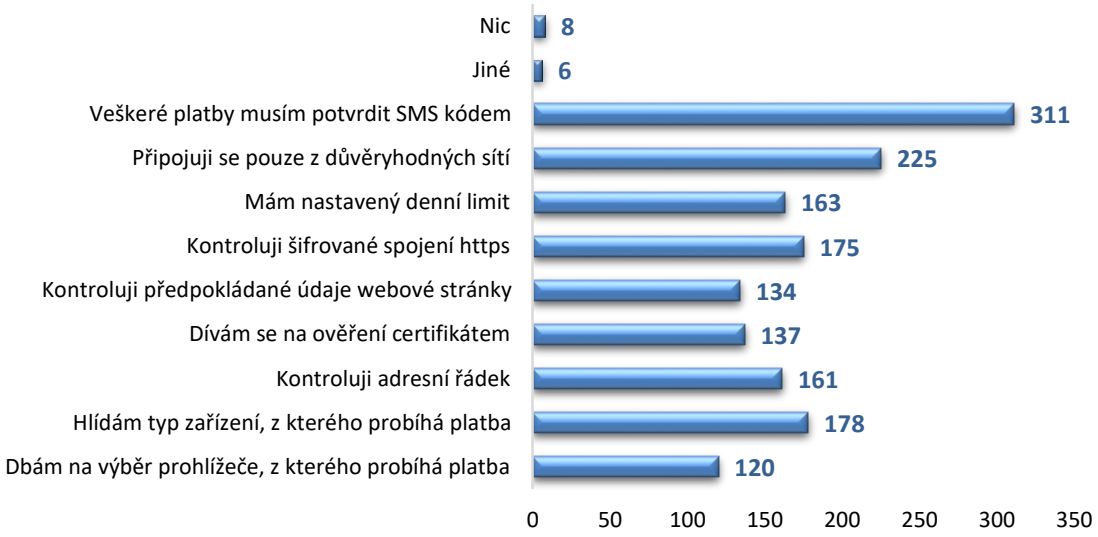


Obr. 13 Frekvence využívání internetového bankovnictví (Otázka č. 7 – Kolikrát jste za poslední 3 měsíce využil/a internetové bankovnictví?)

Další otázka byla cílena na uživatele, využívající internetové bankovnictví. Ptali jsme se konkrétně na bezpečnostní prvky respondentů, využívající ke zvýšení své ochrany před kybernetickým útokem. Překvapující je opověď 8 respondentů, převážně ve věku 16–24 let, jenž uvedli, že pro svou ochranu nepodnikají žádné kroky. Na druhou stranu dobrou zprávou je, že více než polovina respondentů využívá kombinaci minimálně dvou opatření.

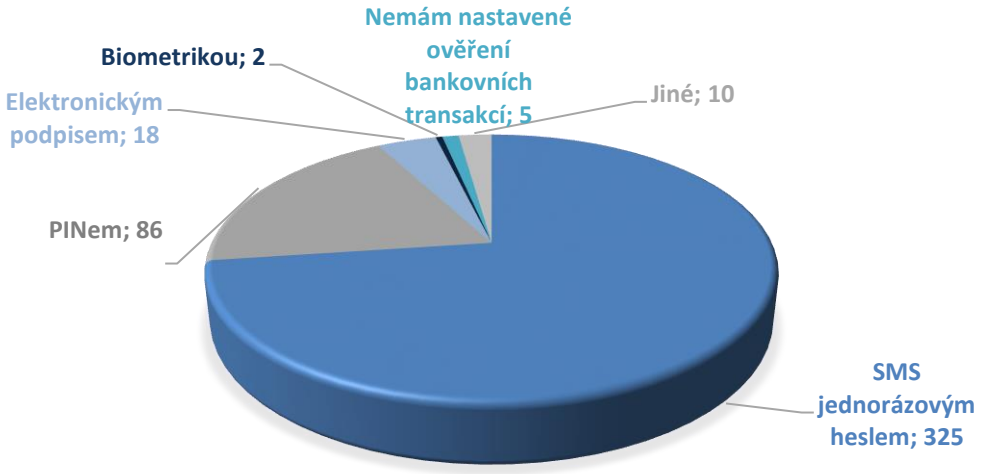
První bariérou proti zneužití, je způsob jak se do internetbankingu přihlašujeme. Můžeme říct, že 178 respondentů z 371 je velice obezřetných při výběru zařízení, z kterého se do svého internetového bankovnictví přihlašuje a celkem 61 % se připojuje pouze z důvěryhodných sítí. Dále bychom chtěli poukázat na fakt, že 120 účastníků výzkumu dbá na výběr prohlížeče. Tyto 3 opatření jsou důležitou součástí každého přihlášení do internetového bankovnictví a měl by jet mít na pozoru každý uživatel. Právě díky připojení z veřejné sítě či skulině v prohlížeči se můžeme stát obětí útočníka. Dalším důležitým bezpečnostním opatřením před provedením jakékoliv platby je kontrola šifrovaného spojení https, jenž si všímá méně než 50 % dotázaných. Když nás útočník přesměruje na stránku se spojením http, kde jsou data přenášena nešifrovaně, může tak sledovat veškerou prováděnou činnost a my můžeme přijít o nemalou částku peněz. To, jestli má stránka v adresním řádku symbol visacího zámku, ověřuje pouze 36 %, celý adresní řádek zkontroluje 161 dotázaných. Další, nejčetnější prvek prevence, vidí 83 % respondentů ve využívání potvrzujícího SMS kódu. Pasivní ochranu ve formě limitů pro platby na svých účtech aplikuje právě 163 dotázaných.

V možnostech odpovědí měli respondenti na výběr i vlastní odpověď. Využilo jí právě 6 účastníků, kteří uvádějí, že mimo výše uvedené využívají k autorizaci bezpečnostní token a autorizační kalkulačku a v rámci své bezpečnosti antivirus.



Obr. 14 Bezpečnostní prvky a opatření při využívání internetového bankovnictví (Otázka č. 8 – Pokud využíváte internetové bankovnictví, co děláte pro svou ochranu?)

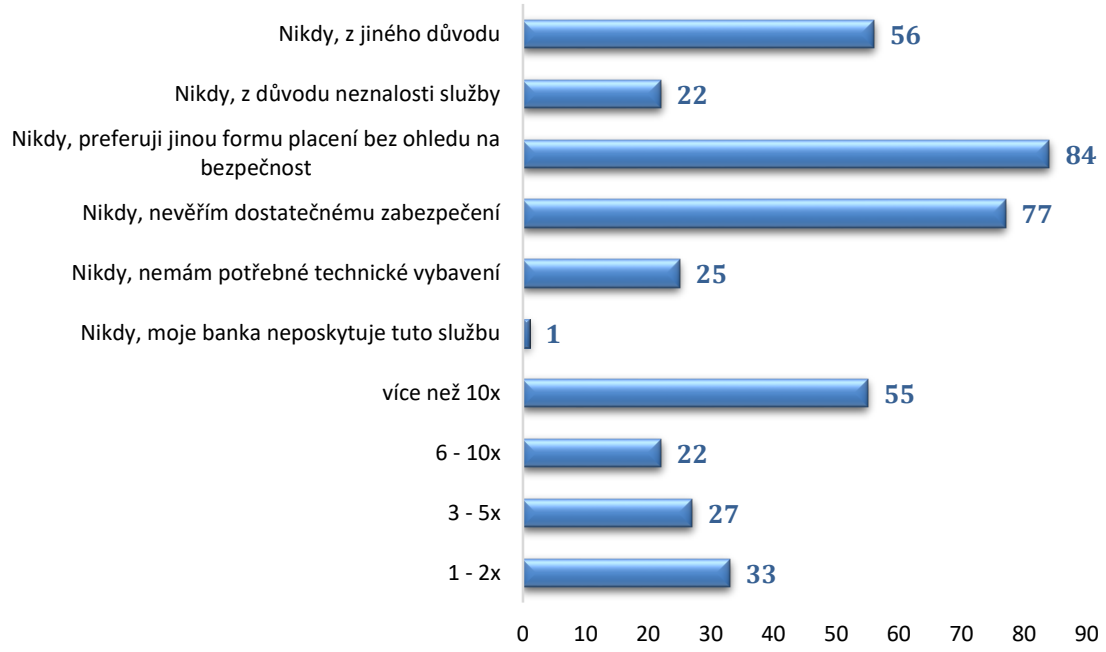
V souvislosti s internetovým bankovnictvím jsme se ptali i na otázku týkající se autorizace bankovních transakcí. V otázce mohli respondenti zaškrtnout více možností odpovědí, z toho důvodu nám nedává celkový součet 371 respondentů, jenž internetové bankovnictví využívá. Jak můžeme vidět na Obr. 14, nejvyužívanější autorizační formou je SMS jednorázové heslo, jež uvedlo 325 účastníků výzkumu. V nabídce odpovědí byla i možnost zvolit vlastní odpověď. Nejčastějšími uváděnými vlastními odpověďmi bylo použití bezpečnostního tokenu a použití osobního klíče ve formě autorizační kalkulačky.



Obr. 15 Autorizace transakcí elektronického bankovnictví (Otázka č. 9 – Jak autorizujete (ověřujete) své bankovní operace v internetovém bankovnictví?)

5.6 Mobilní bankovnictví

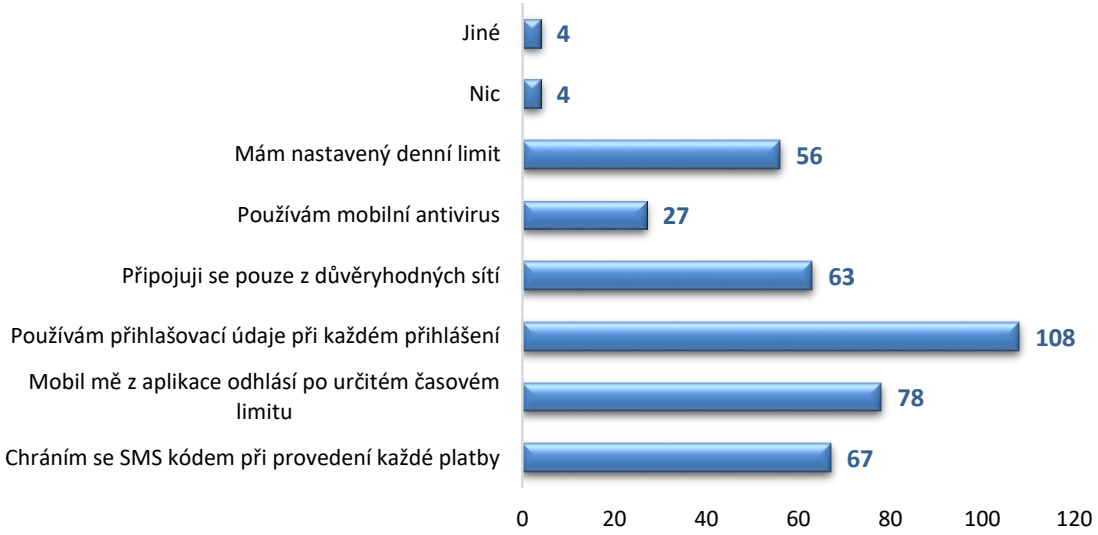
Relativně pestré odpovědi jsme dostali na otázku o frekvenci využívání mobilního bankovnictví. Ze 402 respondentů tohoto dotazníkového šetření jich pouze 34 % tuto službu využívá. Z větší části se jedná o muže. Pro nás je to překvapující odpověď, vzhledem k tomu, že žijeme v době chytrých mobilních telefonů a většina z nás již nedá mobil z ruky. Na druhou stranu bychom si měli přiznat, že ne všichni uživatelé vědí, jak bezpečnost mobilního telefonu zajistit či zvýšit, aby neohrozili finanční obnos, mající na bankovním účtu. O čemž nás přesvědčuje i Obr. 16, ukazující, že právě 77 uživatelů raději mobilní bankovnictví nevyužívá, právě z důvodu nedůvěry v bezpečnost. Nicméně stále nejčetnější odpovědí, kterou zvolilo 21 % dotázaných je, že se bez mobilního bankovnictví lze jednoduše obejít. Vydedukovali jsme to z odpovědi respondentů, kteří preferují jinou formu placení bez ohledu na bezpečnost. Jedná se pravděpodobně o lidi se záporným vztahem k inovacím a moderním technologiím.



Obr. 16 Frekvence využívání mobilního bankovnictví (Otázka č. 10 – Kolikrát jste za poslední 3 měsíce využil/a mobilní bankovnictví?)

Každá banka nabízející mobilní bankovnictví, musí zajišťovat určitou míru zabezpečení, stejně jako u ostatních produktů. Nicméně i přes tento fakt je nutné se věnovat bezpečnosti, která již nespadá do kompetence banky, a kterou může ovlivnit samotný uživatel. Tuto bezpečnost má banka ošetřenou alespoň bezpečnostními zásadami, jenž by měl dodržovat každý uživatel. Avšak dle našeho průzkumu tomu tak rozhodně není.

Mezi obecné zásady bezpečného užívání mobilního bankovnictví patří bezpochyby připojování se pouze z důvěryhodných sítí. I přesto, že se jedná o bezpečnostní zásadu, tak ji dodržuje méně než 50 % uživatelů mobilního bankovnictví. Totéž můžeme říct o mobilním antiviru, kde se dostáváme pouze na 20 % respondentů. Když se podíváme na pasivní formy bezpečnosti, například bezpečnostní limit odhlášení při nečinnosti, můžeme říct, že jej považuje za bezpečnostní prvek a využívá 78 respondentů ze 137.



Obr. 17 Bezpečnostní prvky a opatření při využívání mobilního bankovnictví (Otázka č. 11 – Pokud využíváte mobilní bankovnictví, co děláte pro svou ochranu?)

5.7 Shrnutí platebních prostředků

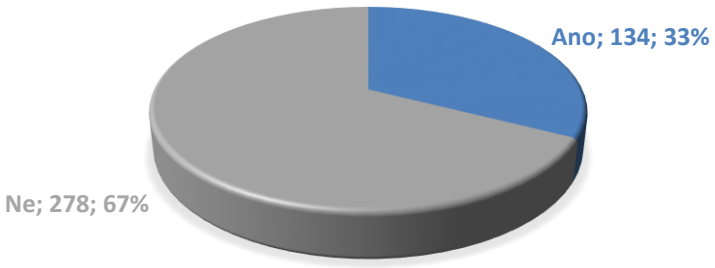
V následující tabulce shrneme a porovnáme frekvenci využívání jednotlivých platebních prostředků, jenž jsme analyzovali v předchozích kapitolách. Jednoznačně nejvyužívanějším platebním nástrojem využívaným k elektronickému platebnímu styku je internetové bankovnictví, jehož podíl využití činí 93 %. Na paty mu šlape platba kartou na internetu, kterou se 78% podílem řadíme na druhé místo. Na další místo spadá mobilní bankovnictví s 34% podílem. Nejméně využívaným nástrojem je platba mobilním telefonem s technologií NFC, zaujímající pouze 3% podíl. Zajímavým zjištěním je fakt, že všechny 4 služby využívá pouze 6 respondentů, a to převážně mužů. Dále bychom chtěli poukázat na to, že 35 % uživatelů internetového bankovnictví využívá také službu mobilního bankovnictví. Našlo se pouze 5 respondentů, kteří využívají mobilní bankovnictví, bez toho aniž by využívali internetové bankovnictví. Z výsledků dotazníkového šetření můžeme také zjistit, že 96 % respondentů, jenž za poslední 3 měsíce alespoň 1x zaplatilo platební kartou na internetu, využívá také internetové bankovnictví a 88 % vlastní bezkontaktní platební kartu. Zbytek respondentů využívá k internetovým platbám kontaktní platební kartu.

Tab. 4 Srovnání frekvencí plateb

	Platba kartou na internetu	Platba mobilním telefonem s technologií NFC	Internetové bankovnictví	Mobilní bankovnictví
1 - 2x	80	2	40	33
3 - 5x	78	0	86	27
6 - 10x	57	2	79	22
více než 10x	98	10	166	55
Nikdy	89	388	31	265

5.8 Elektronické peněženky

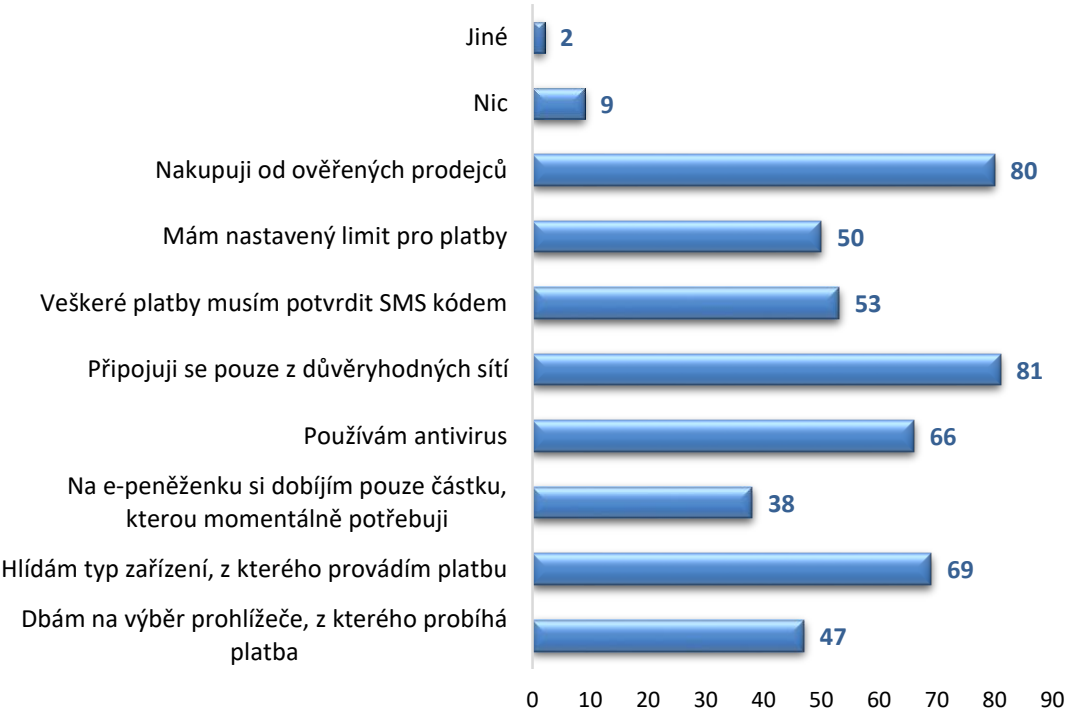
Vzhledem k tomu, že k placení pomocí elektronických peněženek nepotřebujeme vlastnit běžný účet, budeme brát v úvahu i ty respondenty, jenž bankovní účet nemají. Celkový počet respondentů se nám tudíž zvedne z původních 402 na 412, s kterými budeme pracovat i v další sekci s názvem kybernetická kriminalita.



Obr. 18 Využívání elektronických peněženek (Otázka č. 12 – Využíváte platby pomocí elektronických peněženek? (PayPal, Skrill, aj.))

Jak můžeme vidět na Obr. 18 většina respondentů platbu pomocí elektronických peněženek nevyužívá. I když se jedná o nejvyužívanější nebankovní platební systém, respondenti preferují spíše služby bankovní.

Z Obr. 19, jenž se zaměřuje na využívání bezpečnostních prvků při platbě elektronickými peněženkami, můžeme vyčíst, že právě 60 % dbá na výběr důvěryhodné sítě. V těsném závěsu, z hlediska četnosti odpovědí, stojí nakupování od ověřených prodejců. Velkou výhodou elektronických peněženek je nevázanost na běžný účet. Na elektronickou peněženku si nabíjíme pouze tolik peněz, kolik uznáme za vhodné. Nicméně tuto výhodu, v omezenosti nabité částky, v našem výzkumu vidí pouze 38 respondentů. Překvapivě celkem 9 respondentů nevyužívá žádné bezpečnostní opatření a prvky pro snížení rizika napadení.



Obr. 19 Bezpečnostní prvky a opatření využívání elektronických peněženek (Otázka č. 13 – Pokud platíte pomocí elektronických peněženek, co děláte pro svou ochranu?)

5.9 Kybernetická kriminalita

V předchozích kapitolách jsme se zabývali využíváním konkrétních nástrojů elektronického a bezhotovostního platebního styku včetně frekvence placení a aplikováním bezpečnostních opatření a prvků, jenž respondenti využívají ku prospěch své ochrany. Oproti tomu se v rámci této kapitoly zaměříme na povědomí respondentů o riziku spojeném právě s těmito elektronickými platebními prostředky.

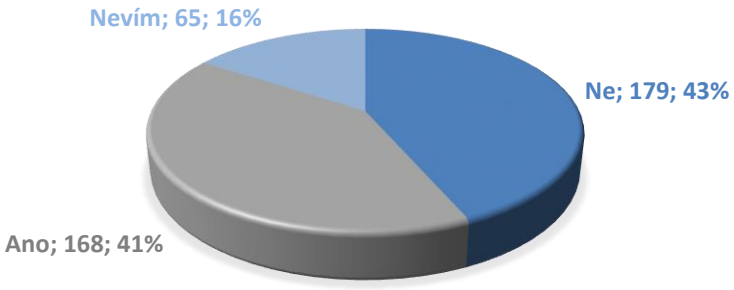
Tab. 5 Odkazy v e-mailu (Otázka č. 14 – Klikáte na odkazy uvedené v e-mailech?)

Věk	Ne	Ano	Příležitostně
16–24 let	49,01 %	7,92 %	43,07 %
25–34 let	49,43 %	5,75 %	44,83 %
35–44 let	53,06 %	6,12 %	40,82 %
45–54 let	48,15 %	3,70 %	48,15 %
55–64 let	54,17 %	8,33 %	37,50 %
65–74 let	65,22 %	4,35 %	30,43 %
Celkový součet	50,73 %	6,80 %	42,48 %

První otázka, znázorněná v Tab. 5 zjišťovala, jestli dotazovaní klikají na odkazy uvedené v emailech. Výsledek této otázky považujeme za pozitivní, protože pouze 6,8 %

účastníků výzkumu potvrdilo, že na odkazy klikne bez jakékoliv obavy. Největší procento neuvážlivých respondentů je mužského pohlaví. Když se na otázku podíváme z opačného hlediska, můžeme říct, že na nespolehlivé odkazy nikdy nekliká přes polovinu dotázaných. 42 % na odkazy kliká příležitostně, podle vlastního uvážení.

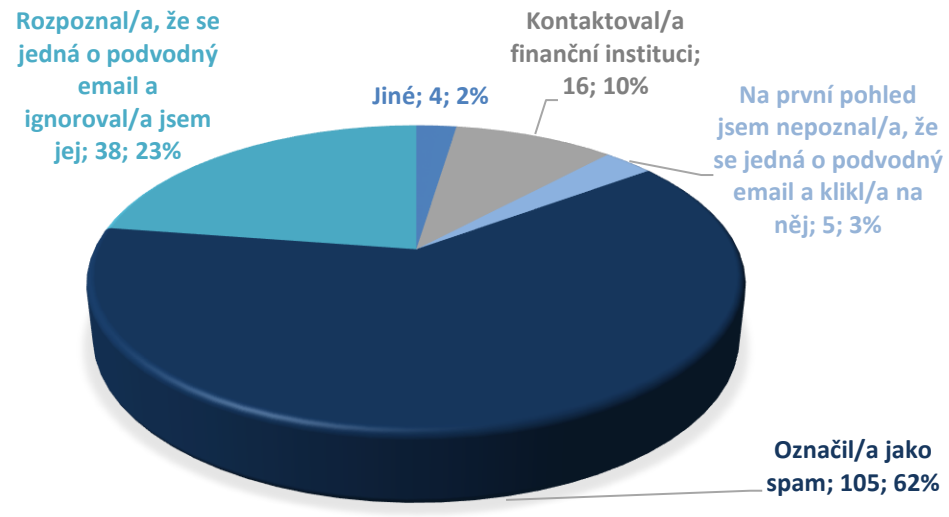
Není žádným překvapením, když se nám do emailové schránky dostane podvodný email zaslaný jménem finanční instituce. Právě na tuto oblast jsme se ptali v rámci další otázky, kde jsme se zjišťovali, zda respondentům někdy přišel podvodný email, který se vydával právě za finanční instituci. Jak můžeme vidět na Obr. 20, 41 % respondentů někdy obdrželo tuto formu podvodné zprávy. Na vybrané procento respondentů se mimo jiné zaměříme v rámci další otázky, kde budeme zjišťovat, jaké učinili další kroky. Jednou z možností výběru v této otázce byla také odpověď *„nevím“,* kterou využilo 65 respondentů. Tato možnost byla do otázky zařazena z toho důvodu, že část lidí pravděpodobně neotevírá poštu od cizích lidí, tudíž ani nemůže vědět, jestli jim tento druh emailu vůbec někdy přišel.



Obr. 20 Podvodný email (Otázka č. 15 – Přišel Vám někdy podvodný email, který se vydával za finanční instituci?)

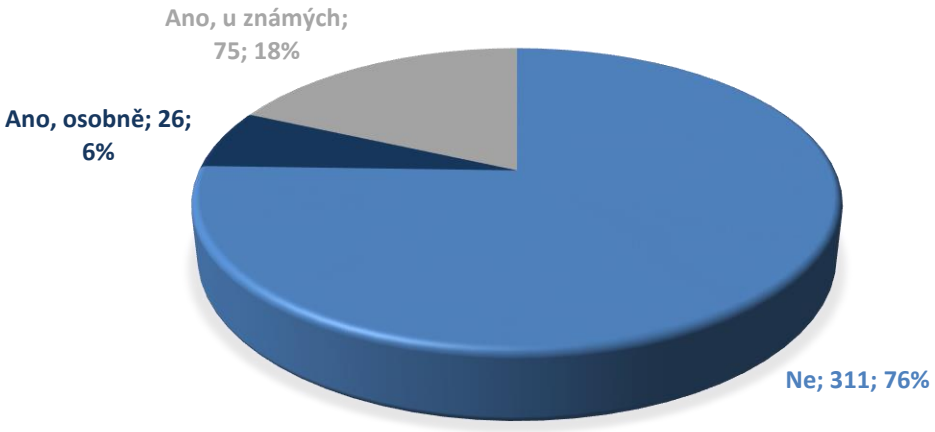
Otázka znázorněná na Obr. 21 s možností více odpovědí, byla zpřístupněna pouze respondentům, jenž v předchozí otázce uvedli, že se s podvodným emailem od odesílatele vydávajícího se za finanční instituci již setkali. Tato část průzkumu ukázala, že se významný podíl respondentů nedokázal adekvátně s příchozím emailem vyrovnat.

Nejlepší postup, jenž můžeme podniknout v případě, že nám přijde podvodný email je kontaktovat finanční instituci a označit email jako spam. Takto učinilo pouze 10 % respondentů s větším podílem mužů než žen. Nicméně tuto odpověď mohl ovlivnit fakt, že respondenti mohli být již svou bankou informováni o šířeném podvodném emailu, proto učinili pouze jediný krok – označili email jako spam. V respondentech se našli i jedinci, jenž nerozeznali podvodný email a klikli na něj. Učinilo tak 5 respondentů ze 168. Jednalo se z větší části o respondenty ve věku 16–24 let. V rámci této otázky mohli respondenti zvolit i vlastní odpověď. Setkali jsme se s odpovědí, že dotyčný tento e-mail ignoroval, protože ho již měl zařazený ve spamové složce od provozovatele e-mailové schránky.



Obr. 21 Způsob vyrovnání se s příchozím emailem (Otázka č. 16 Co jste s takovým emailem udělal/a?)

Z dalšího Obr. 22, zabývajícího se případy reálného setkání se s internetovou kriminalitou, můžeme vyčíst, že právě 26 lidí se s útokem osobně setkalo. Relativně pozitivní zprávou je, že se kriminalita vyhnula obloukem většiny (76 %) respondentů.



Obr. 22 Zkušenost s internetovou kriminalitou (Otázka č. 17 – Setkal/a jste se někdy s internetovou kriminalitou?)

Nyní bychom rádi poukázali na několik vybraných odpovědí otevřené otázky s osobními zkušenostmi respondentů, jenž v předchozí otázce byli mezi 24 %, a odpověděli, že bohužel měli tu možnost se s internetovou kriminalitou někdy setkat.

První zkušenost se stala respondentce v souvislosti se zneužitím platební karty. *„Jednou jsem si objednávala zboží přes internet z ciziny a zaplatila platební kartou*

online. Někdo měl nejspíš hacknuté jejich stránky a stahoval si od nich informace a citlivé údaje o zákaznících. Asi měsíc po uskutečnění této transakce jsem zjistila, že mi z účtu odchází peníze za zboží pořízené v Evropě a Asii, které jsem však neobjednávala já. Okamžitě jsem kartu stornovala a internetové bankovnictví pro jistotu pozastavila. Kartu jsem reklamovala a asi během 2–3 týdnů mi banka peníze vrátila," uvedla respondentka. I přes anonymnost dotazníku můžeme k respondentce přiřadit odpovědi k jednotlivým otázkám, a vyhodnotit tak její bezpečnostní situaci. Víme, že při platbách na internetu pomocí karty využívá 4 bezpečnostní prvky. Dbá na výběr zařízení, používá antivirus, veškeré platby musí potvrdit SMS kódem a má nastavený limit pro platby na internetu. I když se může na první pohled zdát, že respondentka využívá dostatečné zabezpečení, nedodržuje všechny bezpečnostní zásady banky. Jednou z odpovědí byla totiž i možnost výběru *„nakupuji od ověřených prodejců"*, kterou respondentka nezaškrtla. A přesně tato odpověď mohla být důvodem, proč se uživatelka výzkumu nemusela stát obětí kybernetické kriminality.

„Mám od známých příhodu, že si před odletem na dovolenou na letišti vybrali nějakou hotovost. Ale na výpisu se tento výběr objevil 2x. V jednom případě tak, jak měl, a v druhém případě se jednalo o identický záznam ze stejného bankomatu, stejné částky, ale jednalo se o následující den. Nevíme, zda se jednalo o závadu nebo okopírování karty. Každopádně výběr to byl nemožný, protože karta i s majitelem byla tou dobou v jiné zemi. Žádný jiný neoprávněný výběr nebo platba z té karty nebyla. Banka částku vrátila," sdělil další anonymní respondent. Vzhledem k tomu, že se nejedná o příhodu konkrétního respondenta, jenž se zúčastnil našeho výzkumu, nemůžeme tak ověřit, jestli využívající bezpečnostní prvky a opatření jsou dostačující proto, aby se mu nepříjemná událost nepřihodila znovu. Taktéž nemůžeme s jistotou říct, jestli se jednalo o technickou závadu či o skimming, jak uvádí účastník výzkumu.

Další případ se stal respondentce, jenž byla obětí phishingu. *„Přišel mi email, který na první pohled vypadal jako od PayPal, ale byl podvodný a já jsem tam zadala svoje údaje, naštěstí na to banka přišla a tyto platby zablokovala. Dostala jsem novou kartu a na podobné emaily si dávám pozor."* Tato respondentka sice využívá správně vícefaktorovou autentizaci i autorizaci, nicméně opomíjí na největší riziko – lidský faktor. Útočník často využívá lidských vlastností, které se v okamžiku ochrany bezpečnosti stávají slabinami. Komplexní systém zabezpečení pro něj není tak snadný, jako zaměření se na nejslabší článek a ten překonat. Bohužel velice často jím bývá právě člověk. Respondentka by se proto měla zaměřit na vizuální bezpečnostní prvky internetového bankovnictví, mezi něž řadíme převážně kontrolu adresního řádku. Taktéž doporučujeme držet se faktu, že banky nikdy neposílají e-mailem požadavky týkající se citlivých údajů.

Útok phishingu popisuje v rámci dotazníkového šetření více respondentů v různých podobách. Například v dalším případě se jedná o vylákání údajů prostřednictvím sítě Facebook. *„Známý se málem stal obětí podsunutí falešné stránky pro přihlášení do bankovnictví skrz komunikaci přes Facebook s podvodným profilem jinak jemu známé osoby."* Na podobné výzvy bychom neměli nikdy reagovat, a už vůbec ne zadávat přihlašovací údaje do neověřeného odkazu.

„Moje debetní karta (používám ji k fyzickým platbám) byla zneužita někde v zahraničí, platba byla okamžitě zablokována bankou a vydána nová karta. Kreditní kartu (používám pouze na internetu) mi zatím nikdo nezneužil.“ Tento respondent je čistým důkazem toho, že se obětí útoku může stát opravdu každý. I přestože je velice pečlivý a při platbách na internetu dodržuje veškeré bezpečnostní opatření, stal se pravděpodobně obětí skimmingu.

Tab. 6 Postoj k pojištění internetových rizik (Otázka č. 18 - Jaký máte postoj k pojištění internetových rizik?)

Vzdělání	Mám sjednané pojištění	Neznám takové pojištění, proto jej ani nemám	Uvažuji o tomto druhu pojištění	Znám tento druh pojištění, ale nemám o něj zájem
Vysokoškolské	6,58 %	67,76 %	5,92 %	19,74 %
Středoškolské s maturitou	3,37 %	62,98 %	7,69 %	25,96 %
Vyučen v oboru	0,00 %	63,64 %	13,64 %	22,73 %
Základní	0,00 %	90,00 %	0,00 %	10,00 %
Celkový součet	4,13 %	66,75 %	6,80 %	22,33 %

Není tomu tak dávno, kdy pojistitelé přišli na trh s novým produktem zvaným pojištění internetových rizik. Nicméně jak nám dokazuje Tab. 6, většina respondentů, konkrétněji 67 %, takové pojištění vůbec nezná. Může to být způsobeno i faktem, že sjednání pojištění internetových rizik nás nezbavuje odpovědnosti. I přes toto vysoké procento se ve výzkumu našlo 17 respondentů, jenž pojištění využívá. Jednalo se převážně o účastníky s vysokoškolským vzděláním.

Pro zpestření jsme do dotazníku umístili otázku ve formě přiřazovacího kvízu, jež měla ověřit povědomí respondentů o nejčastějších kybernetických útocích bezhotovostního a elektronického platebního styku. Vyskytovaly se zde pojmy phishing, pharming, skimming a carding, na něž odpovědělo správně 41 % respondentů. Když se podíváme na Tab. 6, zjistíme, většina lidí z každé skupiny vzdělání odpověděla špatně. Co nám také vychází z dotazníkové šetření je fakt, že respondenti nejvíce znají pojem carding, k němuž měli přiřadit odpověď *„zneužití platební karty na internetu*“. Správně jej zvolilo 71 % respondentů s větším podílem mužů než žen. Nejvíce si respondenti pletou pojem phishing – *„technika falešného e-mailu napodobující finanční instituci využívaná k získávání citlivých údajů“* a pharming – *„technika, jež přepisuje IP adresu, což způsobí přesměrování klienta na falešné stránky internetbankingu a získá tak citlivé údaje oběti“*. Vzhledem k tomu, že byl phishing nejrozšířenějším útokem na finanční prostředky v roce 2016, očekávali bychom, že jej respondenti znají. Nicméně zjistili jsme, že to není vůbec pravda. Utěšující zprávou je, že i přes velkou chybovost, většina respondentů vždy v rámci možností volby útoku přiřadila správnou odpověď.

Tab. 7 Kvíz (Otázka č. 20)

Vzdělání	Správně	Špatně
Vysokoškolské	43,42 %	56,58 %
Středoškolské s maturitou	42,31 %	57,69 %
Vyučen v oboru	31,82 %	68,18 %
Základní	23,33 %	76,67 %
Celkem	40,78 %	59,22 %

Z provedeného šetření můžeme vyvodit tvrzení, že většina účastníků našeho výzkumu dostatečně nedbá na využívání možné kombinace bezpečnostních prvků a opatření. Předpokládáme, že důvodem je právě malá informovanost respondentů o možných dopadech, kterých si nejsou v dostatečné míře vědomi. Informovanost uživatelů o bezpečnostních rizicích se může zvýšit apelováním na čtení zveřejňovaných zpráv o internetových útocích a incidentech vydávaných finančními institucemi. Tyto zprávy se nám většinou zobrazují při přihlášení do internetového či mobilního bankovnictví a my bychom je neměli brát na lehkou váhu, protože se mohou dotknout v budoucnosti i nás. Také bychom měli dbát na dodržování opatření, jak se takovým útokům vyhnout, popřípadě bránit. Právě tyto sdílené informace bank by měly sloužit jako preventivní nástroj ke snížení kybernetického rizika.

Další mezeru vidíme v samotném vzdělávání uživatelů. Byť je počítačová gramotnost součástí osnov i prvních stupňů základních škol, mělo by být také poukazováno na možná nebezpečí, spojená s jejich užíváním. Vize vzdělávání dětí a mladistvých v kybernetické bezpečnosti je totiž bezesporu jednou z nejaktuálnějších výzev současného školství. Ke zlepšení přístupu k tématu kybernetické bezpečnosti by mohlo přispět vytvoření nových studijních materiálů pro výuku na školách, které by studenty motivovaly ke zvýšení své kybernetické bezpečnosti a to nejen v oblasti platebního styku.

Vyšší informovanosti o kybernetické bezpečnosti by mohly také vypomoct tréninkové moduly a školení pro zaměstnance podniku za podpory zaměstnavatele. I přestože jsou workshopy zaměřené výhradně na únik dat v rámci společnosti, jsou to právě zaměstnanci, jenž se stávají největším terčem útoků. Proto si semináře kladou za cíl ukázat jednotlivcům, jak zabránit situaci, aby se stali obětí a vystavovali tak sebe a své pracoviště potencionálním rizikům. Přínos pro uživatele vidíme ve formě uvědomění si možného rizika a aplikování bezpečnostních opatření a bezpečnostních prvků i v jejich každodenním životě mimo pracoviště.

Taktéž bychom doporučovali zaměřit se na větší propagaci projektů, orientovaných na rizika s používáním internetu, na sociálních sítích. Mluvíme tu například o projektu Bezpečný internet.cz[1] či Národním centru kybernetické bezpečnosti[2], jenž by zveřejňováním informací o vzniklých škodách způsobených kybernetickými útoky mohlo poukázat na závažnost tohoto tématu.

[1] http://www.bezpecnyinternet.cz/

[2] https://www.govcert.cz/

6 Diskuze

V rámci této kapitoly se zaměříme na vzájemnou konfrontaci výsledků dotazníkového šetření, teoretických poznatků a výzkumů podobného charakteru. Tyto porovnání jsou zkoumané v rámci České republiky.

Jako první jsme ve vlastní části práce zkoumali, ihned po specifikaci struktury výběrového souboru, oblast platebních karet. I přes tvrzení ČBA (2016), že oblíbenost těchto karet rok od roku roste na úkor hotovosti, nic nemění na tom, že jednotlivci dostatečně nedbají na své zabezpečení v případě uskutečnění platby. V rámci našeho výzkumu jsme zjistili, že platební kartu za poslední 3 měsíce při platbě na internetu využilo 78 % respondentů, nicméně z toho pouze 73 % autorizuje platby pomocí SMS kódu. Avšak s rozšiřováním služby 3D Secure, kde SMS kód musíme zadat při každé prováděné platbě, předpokládáme, že se podíl respondentů využívající tento bezpečnostní prvek v budoucnosti navýší a sníží se pravděpodobnost rizika útoku.

V rámci šetření nás vůbec nepřekvapily výsledky inovativních možností bezkontaktních plateb. To, že jsou Češi spíše konzervativní, potvrzuje nejenom náš výzkum, ale i průzkum ING, jenž došel k závěru, že se 82 % Čechů v každodenním životě neobejde bez hotovosti. (Němcová, 2017) Také bychom chtěli poukázat na to, že i zaběhlý platební prostředek, platební nálepku, využívá pouze 5 % dotázaných respondentů uskutečněného výzkumu. Na druhou stranu se do České republiky pomalu dostává tzv. wearables. Na to, že nám v šetření pouze 4 respondenti odpověděli, že tuto možnost platby využívají, může mít vliv několik faktorů. Prvním z nich je bezpochyby dostupnost zboží v ČR. Ačkoli chytré hodinky k dostání jsou, o náramku se to říct nedá. Dalším možným faktorem je relativně vysoká cena, která pod 10 tisíc rozhodně nespadá. I přesto, že jsou technologické pokroky fascinující, většina lidí v ČR k nim má spíše skeptický postoj. (Němcová, 2017)

V sekci internetového bankovnictví, jakožto nejvíce využívaného platebního prostředku v rámci plateb na internetu, jsme narazili na problém, že respondenti nedbají na ověření bezpečnosti internetových stránek, z nichž provádí platbu. Z našeho průzkumu vyplynulo, že se pouze 37 % z nich dívá na ověření certifikátem. K malému procentu dospěl i průzkum agentury STEM/MARK, který uvádí 44 % respondentů. Nepatrný rozdíl v procentech u těchto dvou výzkumů může být zapříčiněn strukturou a výběrem respondentů. Doplňující a pro nás překvapující informací je, že se zvýšená opatrnost netýká mladých lidí. Ti dokonce v této oblasti kontroly zabezpečení dopadli nejhůře. (Gordic, 2017)

Další oblasti, mobilnímu bankovnictví, se věnoval i průzkum společnosti ČSOB, jenž došel k závěru, že nejhorší situace je právě v přístupu do bankovnictví z chytrých telefonů. V dle našeho provedeného šetření můžeme říct, že pouze 20 % uživatelů smartbankingu využívá k ochraně antivirový program, což nepovažujeme za uspokojivé. Právě s použitím antiviru se pravděpodobnost usídlení škodlivého souboru v našem mobilním zařízení razantně snižuje. ČSOB také zmiňuje fakt, že pouze 41 % účastníků průzkumu instaluje programy pouze z ověřených zdrojů, čímž se také zvyšuje pravděpodobnost stažení nechtěného softwaru. (Kučera, 2016)

I přesto, že je zajištění kybernetické bezpečnosti jednou z klíčových výzev současné doby, musíme brát stále v úvahu lidský faktor, jenž je tou největší hrozbou při operacích prováděných v rámci platebního styku. Toto tvrzení potvrzují i slova Wolfa, experta na kybernetickou bezpečnost společnosti Gordic, který tvrdí, že nestačí spoléhat na programy, jak si hodně lidí myslí, musíme spoléhat na vlastní hlavu. (Gordic, 2017) Z provedeného šetření vyplynulo, že právě 24 % se někdy s internetovou kriminalitou setkalo, a to není zrovna malý podíl. Tyto respondenty jsme v další otázce žádali o podrobnější popis případů, a došli jsme k závěru, že většina byla založena právě na lidské nepozornosti.

Rádi bychom poukázali také na fakt, že dotazníkové šetření, jenž je základem vlastní části práce, nemůže být bráno jako dogma. I přes využití metodiky Eurostatu, jenž nám s pomocí Metodického manuálu pro tvorbu statistik informační společnosti pomohl k vytvoření vhodného dotazníku, je možné, že je šetření doprovázeno zkreslením a subjektivitou, zapříčiněnou náhodným výběrem respondentů. První ovlivňující faktor je bezpochyby způsob šíření. Vzhledem k tomu, že sběr dat probíhal elektronickou formou, vyloučili jsme tak respondenty, jenž přístup k internetu nevyužívají. Jednalo se převážně o osoby důchodového věku, kteří v dotazníkovém šetření mají zastoupení pouze z malé části. Na druhou stranu většinová skupina ve věku 16–24 let je právě z důvodu publikování dotazníku přes sociální sítě. Pro zajištění úplné reprezentativnosti by bylo třeba snížit počet respondentů ve věkovém rozmezí 16–24 let, a naopak navýšit množství respondentů nad 55 let.

Další zkreslení může být způsobeno odpověďmi respondentů, jenž například uvádí, že dané bezpečnostní opatření dodržují, přitom skutečnost dbaní na bezpečnost je jiná. Je možné, že respondenti přistupovali k vyplnění méně zodpovědně a volili spíše odpovědi, které by se od nich očekávaly, než které jsou pravdivé. Tento faktor ale vyvstává téměř u všech výzkumů totožného typu. Nicméně i přes tyto částečné zkreslení jsme se snažili alespoň o doporučený poměr mužů a žen, daný ČSÚ, který nám pomohl k větší vypovídající schopnosti dotazníkového šetření. Výsledky jsou i přes výše uvedené faktory zpracované objektivně a komplexně. Vzhledem k rozsáhlosti a aktuálnosti daného tématu by bylo možné na tuto práci navázat dalšími výzkumy zaměřujícími se do hloubky na konkrétní bezpečnostní prvky a jejich dodržování v souvislosti s konkrétním platebním prostředkem.

Práci do jisté míry omezovaly dostupné statistické zdroje v rámci České republiky. Jak již bylo v metodické části zmíněno, ČSÚ ani Eurostat se konkrétněji na kybernetickou bezpečnost či využívání bezpečnostních opatření nezaměřuje, tudíž nebylo možné zpracovat informace o povaze reálných případů útoků. Použité data v rešeršní části byly čerpány ze stránek Policie ČR a Národního CSIRT České republiky, jež udávají pouze informace o četnosti jednotlivých útoků za dané časové období. Taktéž konkrétní instituce bankovnictví ponechávají tyto informace pro sebe a vnímají je jako určité tajemství. Tuto mezeru v obsahu produkovaných statistických dat by bylo vhodné vyplnit, a poukázat tak na stupeň závažnosti kybernetických hrozeb.

7 Závěr

První část práce se zaměřovala na současné trendy elektronického a bezhotovostního platebního styku a zkoumala bezpečnostní prvky a opatření běžných uživatelů, které vedou ke snížení kybernetického rizika. Taktéž jsme v ní popsali nejčastější projevy kyberkriminality, s kterými se v souvislosti s touto tématikou můžeme setkat. Okrajově jsme zmínili relativně nový produkt na českém trhu, pojištění internetových rizik, a popsali legislativu, jenž se k problematice bakalářské práce váže. Detailním rozebráním jsme tak splnili jeden z dílčích cílů práce.

Vycházejíce s literární rešerše jsme dle metodických kritérií Eurostatu vytvořili vhodný dotazník k získání dat. Použitou metodikou Eurostatu jsme tak chtěli docílit co nejvíce vypovídajících výsledků. V rámci dotazníkového šetření jsme nasbírali odpovědi od 419 respondentů, které jsme následně dle doporučení očistili od jednotlivců pod 16 let a nad 74 let, a dostali se tak na 412 adekvátních odpovědí. Uskutečněním dotazníkového šetření jsme splnili jeden z dalších dílčích cílů a vypomohli si tím k naplnění cíle hlavního.

Hlavním cílem práce bylo udělat rozbor z nashromážděných výsledků dotazníkového šetření zaměřeného na informovanost veřejnosti o jejich rizicích v dané problematice a zjistit, jaké bezpečnostní prvky a opatření využívají ke zvýšení své bezpečnosti. Tohoto cíle jsme dosáhli v rámci jednotlivých sekcí, kde jsme analyzovali využívání konkrétních nástrojů včetně frekvence placení, ověřili využívání bezpečnostních prvků a opatření a testovali znalost oblasti kybernetické bezpečnosti, čímž jsme splnili i vytyčené záměry dotazníkového šetření. V závěru sekce kybernetické kriminality jsme uvedli doporučení ke zvýšení informovanosti veřejnosti.

Ačkoli banky aktivně usilují o co nejlépe zabezpečený přístup k finančním prostředkům u nich uložených, pachatelé internetové kriminality jsou velmi vynalézaví a dokážou využívat důmyslné techniky k jejich prolomení. Nejslabším článkem, a tedy často největším terčem, jsou pro ně samotní vlastníci bankovního účtu. Nejenom pro banky, ale i pro stát, je rozhodně nejtěžší výzvou vzdělání samotných klientů. Kybernetické riziko je pro většinu lidí stále něco neuchopitelného, něco, pod čím si jen stěží něco představí. Na tento problém jsme narazili převážně u šíření dotazníkového šetření, kdy se nám dostávalo zpětné vazby ve formě komentářů v diskuzních fórech či na sociálních sítích. Většina z nás ví, že jsme za svou kybernetickou bezpečnost z velké části odpovědní, ale nejsme si jisti, jak jí spolehlivě dosáhnout. K lepšímu pochopení problematiky a v závěru i ke snížení kybernetického rizika by měla být nápomocna právě tato bakalářská práce, jež dává veřejnosti ucelené informace o platebních prostředcích a rizicích s nimi spojených. Uživatelé by se také měli sami zamyslet a zejména porozumět tomu, jaké digitální stopy svojí aktivitou v kyberprostoru zanechávají, neboť právě toto poznání jim poskytne nadhled nad rozmanitostí informačních technologií. Rovněž pevně věříme, že informační gramotnost do budoucna poroste a značně tak eliminuje většinu rizik, na internetu číhajících.

8 Seznam použité literatury

ALZA.CZ. Alza.cz varuje před podvodnými SMS. *Alza.cz* [online]. 2017 [cit. 2017-04-01]. Dostupné z: https://www.alza.cz/alzacz-varuje-pred-podvodnymi-sms-

ASOCIACE PRO ELEKTRONICKOU KOMERCI. APEK radí: Desatero bezpečnějšího internetového nakupování. *Asociace pro elektronickou komerci* [online]. 2013 [cit. 2017-03-22]. Dostupné z: https://www.apek.cz/clanky/apek-radi-desatero-bezpecnejsiho-internetoveho-nakupovani

AVG. AVG Technologies unveils global Community Powered Threat Report – Q4-2011. *AVG Technologies* [online]. Amsterdam, 2012 [cit. 2017-03-28]. Dostupné z: http://now.avg.com/avg-technologies-unveils-global-community-powered-threat-report-q4-2011/

BUBÁK, ZDENĚK A VERONIKA DUSOVÁ. Bezkontaktní placení je stále na vzestupu. Platí se nejen kartami, ale i nálepkami a mobily. Přibydou snad i náramky. *Finparáda.cz* [online]. 2017 [cit. 2017-03-26]. Dostupné z: http://finparada.cz/4127-Bezkontaktni-placeni-stale-narusta.aspx?mobile=full

CSIRT.CZ [online]. 2017a [cit. 2017-04-02]. Dostupné z: https://www.csirt.cz/

CSIRT.CZ. Statistiky řešených incidentů. *CSIRT.CZ* [online]. 2017b [cit. 2017-01-12]. Dostupné z: https://www.csirt.cz/page/2635/statistiky-resenych-incidentu/

ČEČELSKÝ, DAVID. Bezpečnost u mobilních zařízení. *PC world security: magazín o bezpečnosti v kybernetickém světě*. Praha: IDG Czech, 2016, 2016(1), 9. ISSN 1802-4505.

ČECH, PETR. *Analýza využívání elektronických platebních prostředků a systémů.* Praha, 2014 [cit. 2017-04-01]. Diplomová práce. Vysoká škola ekonomická v Praze. Vedoucí práce Otakar Schlossberger.

ČERNÝ, ALEŠ. Rok žije s čipem pod kůží. „Rukou" platí za kafe nebo si odemyká počítač. *IDNES.CZ* [online]. 2017 [cit. 2017-03-27]. Dostupné z: http://ekonomika.idnes.cz/profil-cloveka-ktery-ma-v-ruce-nfc-cip-dw5-/ekonomika.aspx?c=A170203_184358_eko_profily_rny

ČESKÁ BANKOVNÍ ASOCIACE. Banky a fakta duben 2017: On-line platby kartami v letech 2013–2016. *Česká bankovní asociace* [online]. 2017 [cit. 2017-05-05]. Dostupné z: https://www.czech-ba.cz/sites/default/files/cba_banky_a_fakta_04-2017_-_on-line_platby.pdf

ČESKÁ BANKOVNÍ ASOCIACE. Banky a fakta listopad 2016: Hotovost, nebo platba kartou? *Česká bankovní asociace* [online]. 2016 [cit. 2017-05-05]. Dostupné z: https://www.czech-ba.cz/sites/default/files/baf_hotovost_vs_karta.pdf

ČESKÁ SPOŘITELNA. Phishing - tiskové zprávy a aktuality: Upozornění na nový phishingový útok. *Česká spořitelna* [online]. 2017b [cit. 2017-04-01]. Dostupné z: https://www.csas.cz/banka/content/inet/internet/cs/sc_18073.xml?archivePage=phishing&navid=nav00156_phishing_aktuality

ČESKÁ SPOŘITELNA. Pololetní zpráva 2016. *Česká spořitelna* [online]. 2016 [cit. 2017-03-30]. Dostupné z: http://www.csas.cz/banka/content/inet/internet/cs/cs_pololetni_zprava_2016.pdf

ČESKÁ SPOŘITELNA. Zásady bezpečného používání Internetbankingu. *Česká spořitelna, a.s.* [online]. ©2017a [cit. 2017-03-27]. Dostupné z: http://www.csas.cz/banka/nav/o-nas/zasady-bezpecneho-pouzivani-internetbankingu-d00014438

ČESKÁ POŠTA. Phishingový útok na klienty České pošty. *Česká pošta* [online]. 2017 [cit. 2017-04-01]. Dostupné z: https://www.ceskaposta.cz/-/phishingovy-utok-na-klienty-ceske-posty

ČSOB [online]. ©2016 [cit. 2016-12-04]. Dostupné z: https://www.csob.cz/

ČSOB. Aktuality. *ČSOB* [online]. 2017 [cit. 2017-04-01]. Dostupné z: https://www.csob.cz/portal/bezpecnost/aktualni-hrozby

ČSOB. Zpráva o činnosti ČSOB za 1. pololetí roku 2016. *ČSOB* [online]. 2016 [cit. 2017-03-30]. Dostupné z: https://www.csob.cz/portal/documents/10710/444804/csob-pololetni-zprava-1h2016.pdf

ČSÚ. Informační společnost v číslech - 2014 - 2016: Kapitola C: Jednotlivci. *Český statistický úřad* [online]. 2017 [cit. 2017-04-04]. Dostupné z: https://www.czso.cz/documents/10180/46014808/061004-17_C.pdf/bc2d28dd-f584-4246-86b8-b34469c91c6b?version=1.1

ČSÚ. Věkové složení obyvatelstva - 2015: Věkové složení obyvatel k 31. 12. 2015. *Český statistický úřad* [online]. 2016 [cit. 2017-02-28]. Dostupné z: https://www.czso.cz/csu/czso/vekove-slozeni-obyvatelstva

DOBDA, LUBOŠ. *Ochrana dat v informačních systémech*. Praha: Grada, 1998. ISBN 80-716-9479-7.

DOČEKAL, DANIEL. Jak se bránit phishingu. *Lupa.cz* [online]. 2008 [cit. 2017-04-20]. ISSN 1213-0702. Dostupné z: http://www.lupa.cz/clanky/jak-se-branit-phishingu/

DOČKALOVÁ, KVĚTA. Tisková zpráva ze zasedání Republikového výboru pro prevenci kriminality. *Ministerstvo vnitra ČR* [online]. 2016 [cit. 2017-04-20]. Dostupné z: http://www.mvcr.cz/webpm/clanek/tiskova-zprava-ze-zasedani-republikoveho-vyboru-pro-prevenci-kriminality-819462.aspx

DOSEDĚL, TOMÁŠ. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

DURAČINSKÁ, ZUZANA. Rok 2016 z pohledu CSIRT.CZ. *SystemOnLine.cz* [online]. 2017 [cit. 2017-04-02]. Dostupné z: https://www.systemonline.cz/it-security/rok-2016-z-pohledu-csirt.cz.htm

DURAČINSKÁ, ZUZANA. Router jako šedé místo v zabezpečení. *PC world security: magazín o bezpečnosti v kybernetickém světě*. Praha: IDG Czech, 2016, 2016(1), 38-39. ISSN 1802-4505.

EUROPEAN COMMISSION. Digital single market: *The strategy. European Commission* [online]. 2016 [cit. 2017-02-28]. Dostupné z: https://ec.europa.eu/digital-single-market/en/the-strategy-dsm

EUROSTAT. Individuals using the internet for internet banking. *Eurostat* [online]. 2016 [cit. 2017-03-30]. Dostupné z: http://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tin00099&plugin=1

FINANČNÍ PORADENSTVÍ ONLINE. Internetové peněženky. Finanční poradenství online [online]. [cit. 2017-01-19]. Dostupné z: https://www.financni-poradenstvi.com/internetove-penezenky/

GOOGLE. Upozornění ve věci ochrany soukromí v prohlížeči Google Chrome. *Google* [online]. 2016 [cit. 2017-01-19]. Dostupné z: https://www.google.com/chrome/browser/privacy/#safe-browsing-policies

GOPAY s.r.o. [online]. ©2016 [cit. 2017-01-19]. Dostupné z: https://www.platebnibrana.cz/

GORDIC. Češi neumí rozpoznat nezabezpečené internetové stránky, navíc riskují s fotkami. *Gordic* [online]. 2017 [cit. 2017-05-05]. Dostupné z: https://www.gordic.cz/zpravy-gordic/2017/cesi-neumi-rozpoznat-nezabezpecene-internetove-str/

GŘIVNA, TOMÁŠ A RADIM POLČÁK, ED. *Kyberkriminalita a právo.* Praha: Auditorium, 2008. ISBN 978-80-9037-867-4.

HÁJKOVÁ, MONIKA. PayPal krok za krokem: Jak jednoduše platit na internetu. *Peníze.cz* [online]. 2014 [cit. 2017-01-18]. ISSN 1213-2217. Dostupné z: http://www.penize.cz/nakupy/293651-paypal-krok-za-krokem-jak-jednoduse-platit-na-internetu

CHRÁSTOVÁ, VERONIKA. *Problematika sociálního inženýrství v souvislosti s elektronickými platebními systémy*. Brno, 2015 [cit. 2017-04-01]. Bakalářská práce. Mendelova univerzita v Brně, Provozně ekonomická fakulta. Vedoucí práce Ing. Stratos Zerdaloglu.

INTEL. Bezpečnost veřejných wi-fi. *Intel* [online]. 2015 [cit. 2017-03-22]. Dostupné z: https://communities.intel.com/community/itpeernetwork/czech-and-slovak/content?filterID=contentstatus%5Bpublished%5D~objecttype~objecttype%5Bblogpost%5D

JAHODÁŘ, MARTIN. *Kybernetické riziko bezhotovostního a elektronického platebního styku*. Praha, 2016 [cit. 2017-04-01]. Bakalářská práce. Vysoká škola ekonomická v Praze. Vedoucí práce Bohumil Stádník.

JANSA, LUKÁŠ, PETR OTEVŘEL, JIŘÍ ČERMÁK, PETR MALIŠ, PETR HOSTAŠ, MICHAL MATĚJKA A JÁN MATEJKA. *Internetové právo*. Brno: Computer Press, 2016. ISBN 978-80-251-4664-4.

JANSSEN, CORY. Cyberattack. *Techopedia™* [online]. [cit. 2017-01-12]. Dostupné z: https://www.techopedia.com/definition/24748/cyberattack

JIROVSKÝ, VÁCLAV. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-802-4715-612.

JUŘÍK, PAVEL. *Svět platebních a identifikačních karet: rady a tipy*. 2. přeprac. vyd. Praha: Grada, 2001. Praxe manažera (Computer Press). ISBN 80-247-0195-2.

KANTNEROVÁ, LIBĚNA. *Základy bankovnictví: teorie a praxe*. V Praze: C.H. Beck, 2016. Beckovy ekonomické učebnice. ISBN 978-80-7400-595-4.

KARTYVBEZPECI.CZ. Bezpečnost bezkontaktní platební karty. *KartyvBezpeci.cz* [online]. [cit. 2017-03-26]. Dostupné z: http://www.kartyvbezpeci.cz/content/9-bezpecnost-bezkontaktnich-platebnich-karet

Kerv [online]. 2017 [cit. 2017-03-26]. Dostupné z: https://kerv.com/en/

KOCMAN, ROSTISLAV A JAKUB LOHNISKÝ. *Jak se bránit virům, spamu, dialerům a spyware*. Brno: CP Books, 2005. ISBN 80-251-0793-0.

KOHOUTOVÁ, ZUZANA. Další banka začala nabízet svým klientům bezkontaktní nálepku. *IDNES.cz* [online]. 2014 [cit. 2017-03-26]. Dostupné z: http://finance.idnes.cz/bezkontaktni-nalepka-csob-09y-/sporeni.aspx?c=A140701_134327_bank_zuk

KOLOUCH, JAN. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7.

KOMERČNÍ BANKA. První na trhu: Bankovní aplikace pro Apple Watch od Komerční banky. *Komerční banka* [online]. 2016 [cit. 2017-03-28]. Dostupné z: https://www.kb.cz/cs/o-bance/tiskove-centrum/tiskove-zpravy/prvni-na-trhu-bankovni-aplikace-pro-apple-watch-od-komercni-banky-2015/

KOSTRECOVÁ, EVA, MATÚŠ JÓKAY A MATEJ KOSTREC. *Počítačová kriminalita*. Bratislava: Nakladateľstvo STU, 2010. Edícia příručiek. ISBN 978-80-227-3410-3.

KOŽÍŠEK, MARTIN A VÁCLAV PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online.* Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

KUČERA, PETR. Nejslabším článkem jste vy, varuje banka klienty. Zjišťovala, jak lidé chrání svůj účet. *Aktuálně.cz* [online]. 2016 [cit. 2017-05-09]. Dostupné z: https://zpravy.aktualne.cz/finance/nejslabsim-clankem-jste-vy-varuje-banka-klienty-zjistovala-j/r~5cef806a16a711e6a77e002590604f2e/

LINUS, ROBIN. *What every Browser knows about you* [online]. [cit. 2017-01-19]. Dostupné z: http://webkay.robinlinus.com/

MÁČE, MIROSLAV. *Platební styk: klasický a elektronický*. Praha: Grada, 2006. Osobní a rodinné finance. ISBN 80-247-1725-5.

MARŤÁK, PAVEL. Bezpečnost dat v praxi. *SystemOnLine* [online]. 2005 [cit. 2017-04-08]. Dostupné z: https://www.systemonline.cz/clanky/bezpecnost-dat-v-praxi.htm

MATĚJKA, MICHAL. *Počítačová kriminalita*. Praha: Computer Press, 2002. ISBN 80-722-6419-2.

MATYÁŠ, VAŠEK A JAN KRHOVJÁK. *Autorizace elektronických transakcí a autentizace dat i uživatelů*. Brno: Masarykova univerzita, 2008. ISBN 978-80-210-4556-9.

MCCARTHY, LINDA A DENISE WELDON-SIVIY, ED. *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online.* Praha: CZ.NIC, 2013. ISBN 978-80-904248-6-9.

MINISTERSTVO FINANCÍ ČR. Výsledky měření úrovně finanční gramotnosti dospělé populace České republiky 2015 [online]. *Ministerstvo financí ČR*, 2016 [cit. 2017-05-02]. Dostupné z: https://www.google.com/url?q=http://www.psfv.cz/assets/cs/media/PSFV_2015_Vysledky-mereni-financni-gramotnosti.pdf&sa=U&ved=0ahUKEwjg4JSD9NHTAhUKPxoKHb2eAUgQFggFMAA&client=internal-uds-cse&usg=AFQjCNHM3wqzut__duLh73WtOYCS7QSLgg

MINISTERSTVO VNITRA ČR. Bezpečnostní hrozby: Kybernetické hrozby. *Ministerstvo vnitra ČR* [online]. Odbor bezpečnostní politiky a prevence kriminality, 2016 [cit. 2017-03-21]. Dostupné z: http://www.mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx?q=Y2hudW09Mw%3D%3D

MONETA MONEY BANK. Pravidla pro bezpečné používání Internet Banky. *MONETA Money Bank* [online]. 2017 [cit. 2017-03-28]. Dostupné z: http://www.moneta.cz/documents/cz/primebankovnictvi/pravidla-bezpecneho-uzivani-ib.pdf

MOZILLA. Jak poznám, zda-li je spojení se serverem zabezpečené? *Mozilla: Mozilla support* [online]. 2017 [cit. 2017-04-02]. Dostupné z: https://support.mozilla.org/t5/Ochrana-soukrom%C3%AD/Jak-pozn%C3%A1m-zdali-je-spojen%C3%AD-se-serverem-za-bezpe%C4%8Den%C3%A9/ta-p/20708

NĚMCOVÁ, VERONIKA. Bez hotovosti se neobejde většina Čechů, ukázal průzkum. *IDNES.CZ* [online]. 2017 [cit. 2017-05-05]. Dostupné z: http://ekonomika.idnes.cz/hotovost-cesi-pruzkum-0bt-/ekonomika.aspx?c=A170428_114726_ekonomika_vem

NIELD, DAVID. The best wearable payment devices: Put the bank card down and pay with your body. *Wearable* [online]. ©2014-2016 [cit. 2017-03-27]. Dostupné z: https://www.wareable.com/wearable-tech/the-best-wearable-payment-devices-976

POLICIE ČR. Skimming. *Policie ČR* [online]. [cit. 2017-01-12]. Dostupné z: http://www.policie.cz/clanek/ncoz-skimming.aspx

POLOUČEK, STANISLAV. *Bankovnictví*. V Praze: C.H. Beck, 2006. Beckovy ekonomické učebnice. ISBN 80-717-9462-7.

PŘÁDKA, MICHAL. *Elektronické bankovnictví: rady a tipy*. Praha: Computer Press, 2000. Praxe manažera (Computer Press). ISBN 80-722-6328-5.

QR platba [online]. [cit. 2017-01-18]. Dostupné z: http://qr-platba.cz/

Sdružení pro bankovní karty [online]. ©2016 [cit. 2016-12-04]. Dostupné z: http://www.bankovnikarty.cz/

SECURE LIST. Financial cyberthreats in 2016. *Kaspersky Lab: Securelist* [online]. 2017 [cit. 2017-04-01]. Dostupné z: https://securelist.com/analysis/publications/77623/financial-cyberthreats-in-2016/

SIMOGLU, ANDREA. Pojištění internetových rizik. *Jak na finance* [online]. 2016 [cit. 2017-02-09]. Dostupné z: http://jaknafinance.eu/pojisteni-internetovych-rizik-v-bezpeci-i-na-internetu

SMRŽ, JIŘÍ. Jawbone představil dva nové chytré náramky. *Dotekomanie.cz* [online]. 2015 [cit. 2017-03-26]. Dostupné z: https://dotekomanie.cz/2015/04/jawbone-predstavil-dva-nove-chytre-naramky/

ŠIMŮNKOVÁ, MONIKA. Riziko kybernetického ohrožení elektronických plateb je v České republice jedno z nejmenších v Evropě. *Finparáda* [online]. 2016 [cit. 2017-03-31]. Dostupné z: http://www.finparada.cz/3704-Riziko-kybernetickeho-ohrozeni-plateb-je-v-Ceske-republice-jedno-z-nejmensich-v-Evrope.aspx

VACCA, JOHN R. *Computer and information security handbook*. Second edition. 2013 [cit. 2017-05-02]. ISBN 978-0123943972.

VISA. Bezkontaktní platby. *Visa* [online]. 2017 [cit. 2017-05-02]. Dostupné z: https://www.visa.cz/zlata-zona/platte-s-visa/bezkontaktni-platby

VOTRUBA, Karel. Přicházejí kybernetické útoky přes chytré televize i lednice. *PC world security: magazín o bezpečnosti v kybernetickém světě*. Praha: IDG Czech, 2016, 2016(1), 28. ISSN 1802-4505.

Wareable [online]. ©2014-2017 [cit. 2017-03-28]. Dostupné z: https://www.wareable.com/

Zákon č. 284/2009 Sb., o platebním styku. In: *Sbírka zákonů České republiky*. 2009, částka 89.

ZEMAN, MIROSLAV. Banky a inovace: Česko je terčem útoků na bankovní účty. *Bankovnipoplatky.com* [online]. 2015 [cit. 2017-04-01]. Dostupné z: https://www.bankovnipoplatky.com/banky-a-inovace-cesko-je-tercem-utoku-na-bankovni-ucty-28069

9 Seznam obrázků

10 Seznam tabulek

Přílohy

A Dotazník

Kybernetické riziko bezhotovostního a elektronického platebního styku
Dobrý den,
ráda bych Vás požádala o vyplnění dotazníku k mé bakalářské práci na Mendelově univerzitě v Brně. Jak název napovídá, dotazník je zaměřen na kybernetické riziko v bankovnictví a bude sloužit ke zpracování vlastní části práce. Vyplnění Vám zabere zhruba 3 minuty. Získané údaje v tomto dotazníku slouží výhradně pro potřeby bakalářské práce.

Děkuji Vám za Váš čas a spolupráci a přeji příjemný zbytek dne.
Kateřina Kuchtová

Máte běžný účet?
- Ano
- Ne

Kolikrát jste platil/a za poslední 3 měsíce platební kartou na internetu?
- 1 – 2x
- 3 – 5x
- 6 – 10x
- Více než 10x
- Nikdy, nevěřím dostatečnému zabezpečení
- Nikdy, moje banka neposkytuje tuto službu
- Nikdy, nemám potřebné technické vybavení
- Nikdy, z důvodu neznalosti služby
- Nikdy, preferuji jinou formu placení bez ohledu na bezpečnost
- Nikdy, z jiného důvodu

Pokud platíte platební kartou na internetu, co děláte pro svou ochranu?
- ☐ Hlídám typ zařízení, z kterého provádím platbu
- ☐ Dbám na výběr prohlížeče, z kterého probíhá platba
- ☐ Připojuji se pouze z důvěryhodných sítí
- ☐ Nakupuji od ověřených prodejců
- ☐ Používám antivirus
- ☐ Kontroluji adresní řádek
- ☐ Kontroluji předpokládané údaje webové stránky (vzhled)
- ☐ Veškeré platby musím potvrdit SMS kódem
- ☐ Mám nastavený limit pro platby na internetu na své kartě
- ☐ Nic
- ☐ Jiné:

Kolikrát jste za poslední 3 měsíce využil/a bezkontaktní platbu mobilním telefonem s technologií NFC?
- 1 – 2x

- 3 – 5x
- 6 – 10x
- Více než 10x
- Nikdy, nevěřím dostatečnému zabezpečení
- Nikdy, moje banka neposkytuje tuto službu
- Nikdy, nemám potřebné technické vybavení
- Nikdy, z důvodu neznalosti služby
- Nikdy, preferuji jinou formu placení bez ohledu na bezpečnost
- Nikdy, z jiného důvodu

Pokud platíte bezkontaktně mobilním telefonem s technologií NFC, co děláte pro svou ochranu?

- □ Mám nastavený limit pro platby
- □ Mám heslo na mobilním telefonu
- □ Používám PIN pro potvrzení platby
- □ Přístup k SIM kartě mám zabezpečen PINem
- □ Platím jen u prověřených prodejců
- □ Nic
- □ Jiné:

Jakou formu bezkontaktní platby využíváte?

- □ Bezkontaktní platební KARTA
- □ Bezkontaktní platební NÁLEPKA
- □ Bezkontaktní platební PŘÍVĚŠEK
- □ Bezkontaktní platební NÁRAMEK
- □ Bezkontaktní platební HODINKY
- □ Mobilní telefon s technologií NFC
- □ Žádnou, nevěřím dostatečnému zabezpečení
- □ Žádnou, moje banka neposkytuje tuto službu
- □ Žádnou, nemám potřebné technické vybavení
- □ Žádnou, z důvodu neznalosti služby
- □ Žádnou, preferuji jinou formu placení bez ohledu na bezpečnost
- □ Jiné:

Kolikrát jste za poslední 3 měsíce využil/a internetové bankovnictví?

- 1 – 2x
- 3 – 5x
- 6 – 10x
- Více než 10x
- Nikdy, nevěřím dostatečnému zabezpečení
- Nikdy, moje banka neposkytuje tuto službu
- Nikdy, nemám potřebné technické vybavení
- Nikdy, z důvodu neznalosti služby
- Nikdy, preferuji jinou formu placení bez ohledu na bezpečnost
- Nikdy, z jiného důvodu

Pokud využíváte internetové bankovnictví, co děláte pro svou ochranu?

- Hlídám typ zařízení, z kterého provádím platbu
- Dbám na výběr prohlížeče, z kterého probíhá platba
- Připojuji se pouze z důvěryhodných sítí
- Dívám se na ověření certifikátem
- Kontroluji šifrované spojení HTTPS
- Kontroluji adresní řádek
- Kontroluji předpokládané údaje webové stránky (vzhledú
- Veškeré platby musím potvrdit SMS kódem
- Mám nastavený denní limit pro platby
- Nic
- Jiné:

Jak autorizujete (ověřujete) své bankovní operace v internetovém bankovnictví?

- SMS jednorázovým heslem
- PINem
- Elektronickým podpisem
- Biometrikou (např. otiskem prstu)
- Nemám nastavené ověření bankovních transakcí
- Nikdy jsem žádnou bankovní operaci neprováděl/a
- Jiné:

Kolikrát jste za poslední 3 měsíce využil/a mobilní bankovnictví?

- 1 – 2x
- 3 – 5x
- 6 – 10x
- Více než 10x
- Nikdy, nevěřím dostatečnému zabezpečení
- Nikdy, moje banka neposkytuje tuto službu
- Nikdy, nemám potřebné technické vybavení
- Nikdy, z důvodu neznalosti služby
- Nikdy, preferuji jinou formu placení bez ohledu na bezpečnost
- Nikdy, z jiného důvodu

Pokud využíváte mobilní bankovnictví, co děláte pro svou ochranu?

- Připojuji se pouze z důvěryhodných sítí
- Používám přihlašovací údaje při každém přihlášení
- Mobil mě z aplikace ohlásí po určitém časovém limitu
- Chráním se SMS kódem při provedení každé platby
- Mám nastavený denní limit pro platby
- Používám mobilní antivirus
- Nic
- Jiné:

Využíváte platby pomocí elektronických peněženek? (PayPal, Skrill, aj.)

- Ano

- Ne

Pokud platíte pomocí elektronických peněženek, co děláte pro svou ochranu?

- ☐ Hlídám typ zařízení, z kterého provádím platbu
- ☐ Dbám na výběr prohlížeče, z kterého probíhá platba
- ☐ Připojuji se pouze z důvěryhodných sítí
- ☐ Nakupuji od ověřených prodejců
- ☐ Používám antivirus
- ☐ Veškeré platby musím potvrdit SMS kódem
- ☐ Mám nastavený limit pro platby
- ☐ Na e-peněženku si dobíjím pouze částku, kterou momentálně potřebuji
- ☐ Nic
- ☐ Jiné:

Klikáte na odkazy uvedené v emailech?

- Ano
- Příležitostně
- Ne

Přišel Vám někdy podvodný email, který se vydával za finanční instituci?

- Ano
- Nevím
- Ne

Pokud Vám přišel podvodný email, co jste s takovým emailem udělal/a?

- ☐ Rozpoznal/a, že se jedná o podvodný email a dále nic nedělal/a
- ☐ Na první pohled jsem nepoznal/a, že se jedná o podvodný email a klikl/a na něj
- ☐ Označil/a jako spam
- ☐ Kontaktoval/a na finanční instituci
- ☐ Podvodný email mi nikdy nepřišel
- ☐ Jiné:

Setkal/a jste se někdy s internetovou kriminalitou v rámci platebního styku?

- Ano, osobně
- Ano, u známých
- Ne

Jaký máte postoj k pojištění internetových rizik?

- Mám sjednané pojištění
- Neznám takové pojištění, proto jej ani nemám
- Znám tento druh pojištění, ale nemám o něj zájem
- Uvažuji o tomto druhu pojištění

Pokud máte zkušenost s internetovou kriminalitou, budu ráda za popsání situace:

Přiřaďte v rámci vašeho uvážení, co si myslíte, že jednotlivé pojmy znamenají

- Phishing technika falešného e-mailu napodobující finanční instituci využívaná k získávání citlivých údajů

- Pharming technika, jenž přepisuje IP adresu, což způsobí přesměrování klienta na falešné stránky internetbankingu a získá tak citlivé údaje oběti
- Skimming technika, při které pachatelé zkopírují údaje z magnetického proužku platební karty bez vědomí držitele karty
- Carding zneužití platební karty na internetu

Pohlaví

- Muž
- Žena

Věk

- Méně jak 16 let
- 16-24 let
- 25-34 let
- 35-44 let
- 45-54 let
- 55-64 let
- 65-74 let
- Víc jak 74 let

Jaké je Vaše nejvyšší dosažené vzdělání?

- Základní
- Vyučen v oboru
- Středoškolské s maturitou
- Vysokoškolské