Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

Rizika elektronického bankovnictví

Michaela Plisková

Bakalářská práce
2019

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2018/2019**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Michaela Plisková**
Osobní číslo:	**E16062**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Rizika elektronického bankovnictví**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Cílem práce je popsat problematiku rizik při využívání online elektronického bankovnictví a nastínit možnosti jejich minimalizace.

Práce bude obsahovat:

- vývoj elektronického bankovnictví;
- typy elektornického bankovnictví;
- bezpečností rizika elektronického bankovnictví;
- možnosti minimalizace rizik.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

PŘÁDKA, Michal a Jan KALA. Elektronické bankovnictví: rady a tipy. Praha: Computer Press, 2000. ISBN 80-7226-328-5.
MATYÁŠ, Vašek a Jan KRHOVJÁK. Autorizace elektronických transakcí a autentizace dat i uživatelů. Brno: Masarykova univerzita, 2008. ISBN 978-80-210-4556-9.
MÁČE, Miroslav. Platební styk: klasický a elektronický. Praha: Grada, 2006. ISBN 80-247-1725-5.
JAMES, Lance. Phishing bez záhad. Praha: Grada, 2007. ISBN 978-80-247-1766-1.

Vedoucí bakalářské práce: **doc. Ing. Pavel Petr, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **3. září 2018**

Termín odevzdání bakalářské práce: **30. dubna 2019**

doc. Ing. Romana Provazníková, Ph.D.
děkanka

L.S.

doc. Ing. Pavel Petr, Ph.D.
vedoucí ústavu

V Pardubicích dne 3. září 2018

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako Školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne Michaela Plisková

PODĚKOVÁNÍ:

Tímto bych chtěla poděkovat doc. Ing. Pavlu Petrovi, Ph.D. za cenné připomínky a odborné rady při konzultacích mé bakalářské práce. Také bych chtěla poděkovat mojí rodině za jejich podporu.

ANOTACE

Tato bakalářská práce je zaměřena na rizika elektronického bankovnictví, jejich popis, vysvětlení a možnosti, jak tato rizika minimalizovat. Práce je rozdělena do pěti hlavních kapitol. První tři kapitoly popisují elektronické bankovnictví a jeho bezpečnostní mechanismy. V posledních dvou kapitolách jsou popsána rizika elektronického bankovnictví a možnosti jejich minimalizování.

KLÍČOVÁ SLOVA

elektronické bankovnictví, bezpečnostní mechanismy, phishing, malware, biometrie

TITLE

Risks of electronic banking

ANNOTATION

This bachelor's thesis is focused on the risks of electronic banking, their description, explanation and possibilites how to minimize them. Thesis is divided into five main chapters. The first tree chapters describes electronic banking and its sefety mechanisms. Last two chapters describes the risks of electronic banking and possibilities how to minimize them.

KEYWORDS

electronic banking, safety mechanisms, phishing, malware, biometrics

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM GRAFŮ

SEZNAM TABULEK

SEZNAM ZKRATEK A ZNAČEK

USA	United States of America (Spojené státy Americké)
USD	United States dollar (Americký dolar)
NFC	Near Field Communication
GSM	Groupe Spécial Mobile (Globální Systém Mobilní komunikace)
WAP	Wireless Application Protocol (Aplikační protokol pro bezdrátová zařízení)
ISO	International Organization for Standardization
EMV	Europay, MasterCard a Visa
CVV	Card Verification Value
CVC	Card Verification Code
PIN	Personal Identification Number (osobní identifikační číslo)
ČR	Česká republika
Kč	Korun českých
ATM	Automated teller machine (bankomat)
SEPA	Single euro payments area (Jednotná oblast pro platby v eurech)
SIM	Subscriber identity module (účastnická identifikační karta)
OTP	One Time Password (jednorázové heslo)
SMS	Short message service (krátká textová zpráva)
DNA	Deoxyribonucleic acid (deoxyribonukleová kyselina)
FAR	False Acceptance Rate (chybné přijetí)
FRR	False Rejection Rate (chybné odmítnutí)
3D	Three-dimensional space (trojdimenzionální)
MFA	Multi-Factor Authentication (multifaktorové ověření)
2FA	Two-factor Authentication (dvoufaktorové ověření)
PKI	Public Key Infrastructure
CA	Certificate authoriy
TSL	Transport Layer Security
SSL	Secure Socket Layer
HTTPS	Hypertext Transfer Protocol Secure
HTTP	Hypertext Transfer Protocol
ASP	Active Server Pages
PHP	Hypertext Preprocessor
ČSOB	Československá obchodní banka
DNS	Domain Name System

IP	Internet Protocol
DVD	Digital Versatile Disc
USB	Universal Serial Bus
Wi-Fi	Wireless Fidelity
ePIN	electronical Personal Identification Number

ÚVOD

Elektronické bankovnictví je využíváno hlavně pro jeho jednoduchost a pohodlnost. Uživatel elektronického bankovnictví má své peníze k dispozici ihned, k vyzvednutí hotovosti mu stačí návštěva bankomatu, který na rozdíl od banky nemá otevírací hodiny. Tyto a další výhody s sebou ale přinášejí i jistá rizika. Právě tato rizika jsou hlavním tématem této bakalářské práce.

V úvodu této práce je důležité zmínit, že nepokrývá všechny oblasti daného tématu, ale pouze ty nejdůležitější, a to z důvodu jejího rozsahu. Rizika elektronického bankovnictví jsou velice rozsáhlé téma, které se neustále vyvíjí, protože se stále objevují nová rizika a zločinci nacházejí nové způsoby. Na druhou stranu se ale i zvyšuje zabezpečení bankovních účtů, čímž se rizika snižují.

Tato práce je rozdělena do pěti hlavních kapitol. Pro lepší pochopení celého elektronického bankovnictví je první kapitola věnována historii elektronického bankovnictví. V této kapitole je pohled na vznik elektronického bankovnictví ve světě a v České republice. V druhé kapitole jsou uvedeny jednotlivé druhy elektronického bankovnictví a jejich možnosti. Třetí kapitola obsahuje bezpečnostní mechanismy, především ty, které jsou používány pro ověření uživatele, dále ale i bezpečnostní mechanismy internetových stránek. V následující kapitole jsou pak uvedena rizika spojená s používáním elektronického bankovnictví. V poslední kapitole jsou uvedeny možnosti, jak je možné tato rizika minimalizovat.

Cílem práce je nalézt a popsat vybraná rizika elektronického bankovnictví a najít možnosti, jak se tato rizika dají minimalizovat.

Po přečtení této práce by měl být uživatel elektronického bankovnictví seznámen s nejčastějšími riziky, které se spolu s elektronickým bankovnictvím objevují, byl schopný tato rizika odhalit a minimalizovat jejich vznik.

1 HISTORIE ELEKTRONICKÉHO BANKOVNICTVÍ

Pro lepší přestavení a pochopení daného tématu je dobré podívat se do historie elektronického bankovnictví. V této kapitole je pohled do celosvětové historie elektronického bankovnictví, především do USA, a na začátky elektronického bankovnictví v České republice.

1.1 Historie elektronického bankovnictví ve světě

Není pochyb o tom, že nejstarší formou elektronického bankovnictví jsou platební karty. První platební karta se objevila v USA v roce 1914, kdy společnost Western Union Telegraph Company poskytovala svým klientům úvěrovou kartu, kterou bylo možné platit za telefonáty a zasílání telegramů. Na konci měsíce pak přišlo klientovi vyúčtování. Významnou událostí ve světě platebních karet byl však vznik platební karty, se kterou se dalo platit na více místech; v restauracích, hotelech nebo v obchodech. Za vznik této karty je zodpovědný Frank McNamar, podle jehož názoru by se lidé ve svém utrácení neměli omezovat hotovostí, kterou nosí u sebe. Takto vznikla roku 1949 Diners Club Card. [1]

V roce 1958 se o zavedení platebních karet pokoušely bankovní společnosti, které se ale ze začátku shledaly s velkým neúspěchem, protože klienti nespláceli své úvěry a samotné platební karty se kradli už při jejich výrobě, protože banky neověřovali totožnost jejich vlastníka a bylo velmi snadné je zneužít. Ztráty při zavádění platebních karet podle odhadu stály přibližně 115,5 mil. USD. Pro snížení šancí padělat kartu přibyl na platebních kartách magnetický proužek, který obsahoval informace o držiteli karty a účtu, ke kterému byla karta vedena. Takto vybavená karta se objevila roku 1969 a o 4 roky později mělo magnetický proužek 85 % všech platebních karet. [2]

Historie elektronického bankovnictví, prováděného pomocí počítače, sahá do období 80. let 20. století, konkrétně do roku 1981, kdy v USA začaly tyto služby testovat hned čtyři banky. O dva roky později první z nich začala své služby nabízet zákazníkům, jednalo se o banku Chemical Bank, která umožňovala přes počítač a telefonní linku kontrolovat zůstatek na účtu, spravovat elektronicky šekové knížky, prohlížet historii plateb a zadávat online platby obchodníkům. [3]

V 90. letech minulého století se začalo rozvíjet elektronické bankovnictví pomocí internetu. Bylo však důležité, aby internetové spojení mezi bankou a klientem bylo bezpečné. První řešení, které zajišťovalo bezpečnost přenosu informací, byl homebanking. Nevýhodou tohoto řešení byla nutnost instalování softwaru na konkrétní počítač. [3]

První zprostředkování elektronického bankovnictví prostřednictvím webového prohlížeče bylo nabídnuto ve Spojených státech amerických v říjnu 1994. Od roku 1995 pak vznikaly i banky, které fungovaly jen prostřednictvím internetu a neměly žádné pobočky, tyto banky se však příliš neuchytily a ve většině případů zanikly nebo byly odkoupeny většími společnostmi, které ovšem nefungovaly pouze online, ale měly i své pobočky. To ovšem neměnilo nic na tom, že samotné elektronické bankovnictví se prostřednictvím internetu používalo čím dál tím častěji. Především ve Spojených státech amerických, kdy v roce 2000 nabízelo internetové bankovnictví 80 % všech bankovních společností. [2]

1.2 Historie elektronického bankovnictví v České republice

Do České republiky přišlo celé elektronické bankovnictví se značným zpožděním. První Československá banka, která poskytovala platební karty, byla Živnostenská banka. Do 80. let 20. století tuto kartu mohli využívat pouze lidé, kterým bylo umožněno pracovat v zahraničí. Zlom nastal po roce 1989, kdy začalo vznikat množství bankovních institucí, které se snažily získat co nejvíce klientů, nabízely proto spoustu nových služeb včetně platebních karet. K této příležitosti bylo také nutné uvést do provozu bankomaty, aby si lidé mohli vybírat svou hotovost. Obchodníci začali přijímat platební karty, nejdříve tyto platby probíhaly offline. Při těchto platbách bylo nutné telefonicky ověřit zákazníka a prostřednictvím imprinteru vyrobit platební příkaz. Později se rozšířily platební terminály, prostřednictvím kterých bylo možné provádět platby elektronicky. Placení platebními kartami se stále vyvíjí, v posledních pár letech se objevila, dnes již velmi rozšířená, možnost provádět bezkontaktní platby, nebo také platit mobilním telefonem. [4]

V České republice první internetové bankovnictví nabízela v roce 1998 Rodinná záložna. Více známá byla pro své elektronické bankovnictví ve stejném roce i Expandia Banka, známá spíše jako eBank, která na svou dobu nabízela svým klientům množství služeb, jako je internetové bankovnictví, telefonní bankovnictví, a další. Následně tyto služby začaly nabízet i ostatní banky a postupně se elektronické bankovnictví vyvíjí až dodnes. [3]

2 TYPY ELEKTRONICKÉHO BANKOVNICTVÍ

Typů elektronického bankovnictví existuje celá řada, některé se do České republiky ani nedostaly, jiné ano, ale už se nepoužívají. Mezi dnes nejrozšířenější patří platební karty, internetové bankovnictví a smart bankovnictví, tyto a další významné typy jsou popsány v této kapitole. [5]

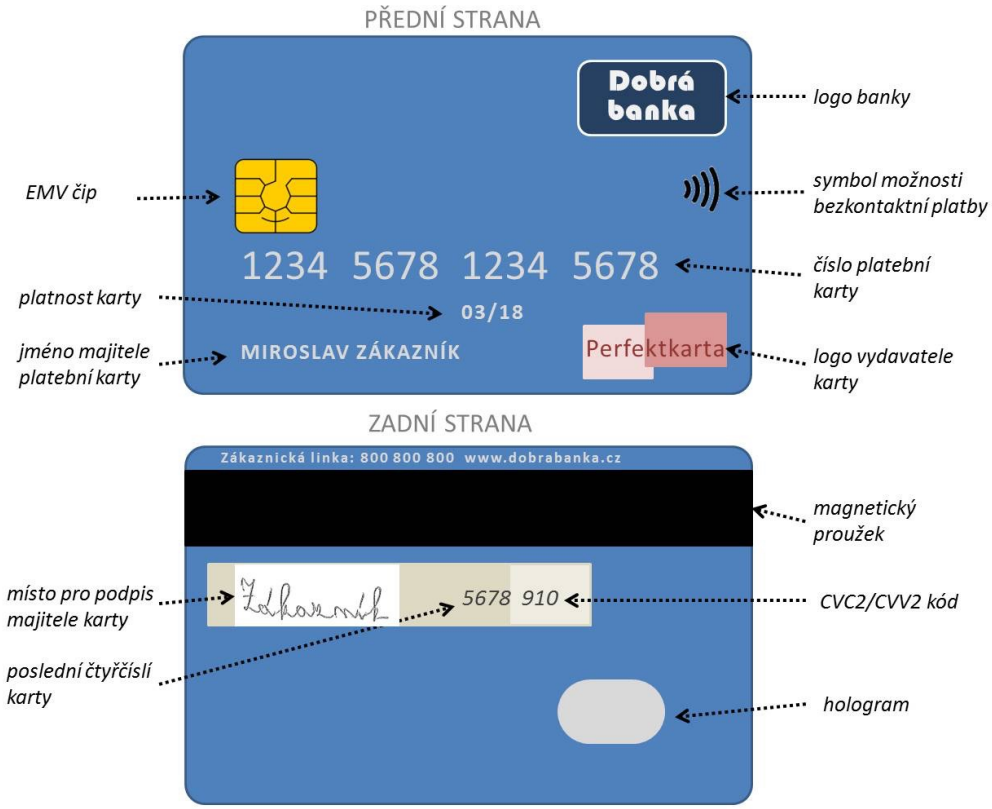
Typy elektronického bankovnictví uvedené v této práci:

a) platební karty;
b) homebanking;
c) internetové bankovnictví;
d) smart banking;
e) telefonní bankovnictví;

a) Platební karty

Platební karty jsou bezpochyby nejvyužívanější druh elektronického bankovnictví. V některých zdrojích k elektronickému bankovnictví platební karty neodmyslitelně patří, v jiných je tomu naopak, a to hlavně z důvodu, že platební karta má pouze dvě funkce: platit a vybírat hotovost z bankomatů. Dle mého názoru pod elektronické bankovnictví rozhodně spadají, zvláště pak v dnešní době, kdy je možné si platební kartu pomocí Google Pay, Apple Pay nebo dalších služeb nahrát do telefonu a platit tak přímo chytrým telefonem. [6]

Fyzická platební karta je identifikační doklad. Rozměry a fyzikální vlastnosti platebních karet stanovuje mezinárodní norma ISO 3554. Na platební kartě je několik základních prvků; číslo karty, EMV čip, období platnosti, jméno držitele karty, magnetický proužek, podpisový proužek a CVV/CVC. Jejich podobu a umístění můžeme vidět na obrázku 1. [7]



Obrázek 1: Platební karta

Zdroj:[8]

EMV čip se nachází na tzv. čipových nebo-li hybridních kartách. Hybridní a čipové karty jsou to samé, protože podle standardu EMV karta musí obsahovat čip i magnetický proužek. EMV čip je mikroprocesor, který stejně jako magnetický proužek obsahuje informace o platební kartě, navíc má však tento čip i procesor a rozhraní, kterým zvládne aktivně komunikovat s platebním terminálem. [9]

Číslo karty se skládá ze šestnácti číslic, první dvě číslice určují druh karty (např. Visa nebo Mastercard), dalších pět číslic banku a zbývajících devět čísel identifikuje samotného uživatele platební karty. [7]

CVV/CVC je třímístný kód, který se kvůli bezpečnosti nachází na zadní straně karty. Je využíván u všech internetových plateb, v případech, kdy nelze vyžadovat PIN karty a kdy není karta fyzicky přítomna. [10]

Existují tři základní druhy platebních karet [11]:

- **debetní karta** – je v České republice nejrozšířenější. Při použití debetní karty čerpáte peníze přímo z vašeho účtu
- **kreditní karta** – při použití kreditní karty čerpáte kredit, který vám poskytuje banka, a tento kredit pak bance vracíte z peněz, které jsou na vašem účtu

- **charge karta** – funguje na podobném principu jako karta kreditní. Máte stanovený obnos peněz, které vám půjčuje banka, jednou za určitou časovou dobu vám přijde vyúčtování za všechny čerpané položky a toto vyúčtování pak zaplatíte z vašeho účtu.

Bezkontaktní platební karty

Dnes již běžným druhem platebních karet jsou bezkontaktní platební karty. Jejich rozšíření v ČR je poměrně rozsáhlé. Bezkontaktní transakce tvořily v roce 2018 85 % z celkového počtu transakcí. Z pohledu vydaných karet v roce 2018 tvoří bezkontaktní platební karty 95 % ze všech nově vydaných platebních karet. [14]

Tyto karty jsou vybaveny NFC technologií. NFC (Near Field Communication) je technologie, která dovoluje bezdrátovou komunikaci mezi zařízeními, které jsou od sebe pár centimetrů vzdálené. Existují dva druhy NFC, pasivní a aktivní. Pasivní NFC nepotřebuje ke svému fungování elektrickou energii. To jsou například kreditní karty nebo štítky, druhým druhem je aktivní NFC, tyto zařízení potřebují elektrickou energii a na rozdíl od pasivních dokáží data nejen vysílat, ale i přijímat. [12]

Pro přenos dat není zapotřebí internetové připojení, místo toho využívá mikročip pro přenesení dat přes krátkovlnné rádiové frekvence. NFC mikročip v bezkontaktní platební kartě umožní sdělit platební údaje čtečce bezkontaktních karet, čímž je provedena samotná platba. [12]

Pro zvýšení bezpečnosti je u plateb, které překročí určitou částku vyžadováno potvrzení zadáním PIN kódu. V České republice je touto hranicí 500 Kč. [13]

Platební karty v telefonu

Provádění plateb pomocí telefonu je možné díky technologii NFC. Placení funguje velice podobně jako bezkontaktní placení platební kartou. V letošním roce se placení mobilním telefonem rozrostlo díky službě Apple pay, která se dostala do České republiky a začala být nabízena několika bankami. Apple pay ale není jedinou službou, díky které se dá platit pomocí mobilního telefonu. Dalšími službami jsou Google pay, Samsung pay, aplikace, které jsou navržené jednotlivými bankami a další. Platební kartou v telefonu je možné platit všude, kde je možné platit bezkontaktní platební kartou. [15]

b) Homebanking

Homebanking je předchůdce internetového bankovnictví známého z dnešní doby. Díky jeho vysokému stupni zabezpečení byl využíván hlavně na konci 20. století, kdy nebyla

k internetovému bankovnictví velká důvěra. Dnes však již internetové bankovnictví homebanking kompletně nahradilo.[16]

Prostřednictvím homebankingu bylo možné provádět transakce a v reálném čase sledovat pohyby na účtu. To vše zprostředkovává software s informačním systémem banky, který lze ale nainstalovat jen na jeden, nebo na skupinu určitých počítačů. Nevýhodou domácího bankovnictví byla právě vázanost na tyto počítače, protože software nebylo možné přehrát na jiný počítač. Další nevýhodou byla také pořizovací cena, která byla vyšší než u ostatních druhů elektronického bankovnictví. [17]

Výhodou homebankingu je už zmiňovaný vysoký stupeň zabezpečení. Bezpečnost a ochrana přenosu dat je zajišťována metodami šifrovacích klíčů, uživatelských hesel, algoritmů a elektronických podpisů. [16]

c) Internetové bankovnictví (internet banking)

Dnes se jedná o druhý nejrozšířenější druh elektronického bankovnictví. Na rozdíl od homebankingu internetové bankovnictví nepotřebuje ke svému chodu žádný software, díky čemuž se stává mnohem dostupnější. [18]

K připojení do internetového bankovnictví je potřeba počítač, mobilní telefon nebo tablet s připojením k internetu a obyčejný internetový prohlížeč. Po přihlášení do internetového bankovnictví může klient rovnou zadávat pokyny bance. [19]

Operace, které se dají provádět v internetovém bankovnictví, se liší podle konkrétní banky. Většina bank však v dnešní době poskytuje systémy internetového bankovnictví, které téměř zcela umí nahradit přístup do banky, protože přes ně lze provést většinu bankovních operací. [18]

d) Smart banking

Smart banking funguje velmi podobně jako internetové bankovnictví a nabízí ho většina českých bank. Rozdílem mezi internetovým bankovnictvím a smart bankingem je ten, že smart banking funguje prostřednictvím aplikace v chytrém mobilním telefonu. Smart banking je čím dál tím více využívaná služba. Mezi hlavní jeho výhodu patří dostupnost. Prostřednictvím smart bankingu se dá mimo jiné sledovat pohyby na účtu, aktuální zůstatek, nebo provádět platby. [20]

e) Telefonní bankovnictví

Telefonní bankovnictví je, hned po platebních kartách, druhý nejstarší typ elektronického bankovnictví. Dnes se již tak hojně nevyužívá, ale stále se najdou v České republice banky, které tuto službu nabízí, například ČSOB nebo Komerční banka. Telefonní bankovnictví funguje tak, že klient zavolá do své banky, kde je spojen s automatem a pomocí tlačítek na telefonu si může vybrat požadovanou službu, např. dotaz na zůstatek na účtu. V případě, že si z dané nabídky nevybere, je přesměrován k pracovníkovi banky a svůj požadavek řeší přímo s ním. [21]

3 BEZPEČNOSTNÍ MECHANISMY

Bezpečnostní mechanismy jsou algoritmy, které softwarově nebo hardwarově implementují nějakou bezpečnostní funkci. Bezpečnostních mechanismů je spousta, v této práci jsou uvedeny pouze ty nejpoužívanější v oblasti zabezpečení elektronického bankovnictví. V této kapitole jsou bezpečnostní mechanismy rozděleny do dvou skupin. První částí jsou bezpečnostní mechanismy pro ověření uživatele, druhou pak bezpečnostní mechanismy internetové stránky. [22]

3.1 Bezpečnostní mechanismy pro ověření uživatele

Ověření uživatele se provádí, aby se předešlo neoprávněnému přístupu do jakéhokoliv systému. Tyto bezpečnostní systémy v elektronickém bankovnictví zamezují neautorizovaným a neoprávněným platebním transakcím. [23]

Často využívanými bezpečnostními mechanismy pro ověření uživatele jsou:

a) heslo;
b) jednorázové heslo;
c) biometrie;
d) dvoufaktorová a multifaktorová autentizace;

a) Heslo

Hesla jsou v elektronickém bankovnictví dnešní doby nejrozšířenější formou ověření uživatele. Bezpečnost hesla je dána jeho složitostí, čím je heslo složitější, tím je bezpečnější. Složitostí hesla se rozumí jeho délka a použité znaky, podrobněji je tato problematika popsána níže. Heslo by nemělo mít spojení s osobním životem, tzn. nemělo by obsahovat jména domácích mazlíčků, životních partnerů, datum narození apod. [24]

Možnosti útočníka získat cizí heslo jsou různé. Může to být přesvědčením osoby, aby mu heslo poskytla, další metodou je vymámení hesla od osoby nenápadným způsobem, může se jednat např. o phishing, kterému se budu ve své práci věnovat později. Další metodou je tzv. slovníkový útok, kdy si útočník stáhne z internetu balíčky, které obsahují nejpoužívanější hesla, u kterých vyzkouší, jestli jedno z nich není jeho oběti. Poslední z metod je metoda hrubou silou, kdy útočník použije algoritmus, který postupně zkouší všechny možné variace hesel tak, že skládá jednotlivé znaky za sebe do té doby, než nenajde správnou kombinaci, kterou uloží a útočník ji pak může použít. V tomto posledním případě je složitost hesla nejdůležitější. V tabulce 1 je znázorněn počet kombinací, které musí algoritmus projít, aby nalezl požadované heslo. [25]

Tabulka 1: Počet možností hesla

	Č	M	Č+M	Č+M+V	Č+M+V+S
3 znaky	1 000	17 576	46 656	238 328	857 375
5 znaků	100 000	12 mil	60 mil	916 mil	7 miliard
10 znaků	10^{10}	26^{10}	36^{10}	62^{10}	95^{10}

Zdroj: vlastní zpracování

Legenda:

Č = číslo
M = malé písmeno
V = velké písmeno
S = symbol

Každý algoritmus na prolomení hesla pracuje jinak rychle. Pro ukázku, jak časově náročné prohledávání je, budu pracovat s hodnotou 10 miliónů porovnání a vyhodnocení za vteřinu. Tabulka 2 pak ukazuje, jak dlouho by trvaly jednotlivé kombinace hesel prolomit. Je důležité podotknout, že počet těchto porovnání a vyhodnocení za určitou časovou jednotku se liší v závislosti, na jakém zařízení a jakým způsobem se útočník snaží heslo prolomit. [25]

Tabulka 2: Časová náročnost pro odhalení hesla

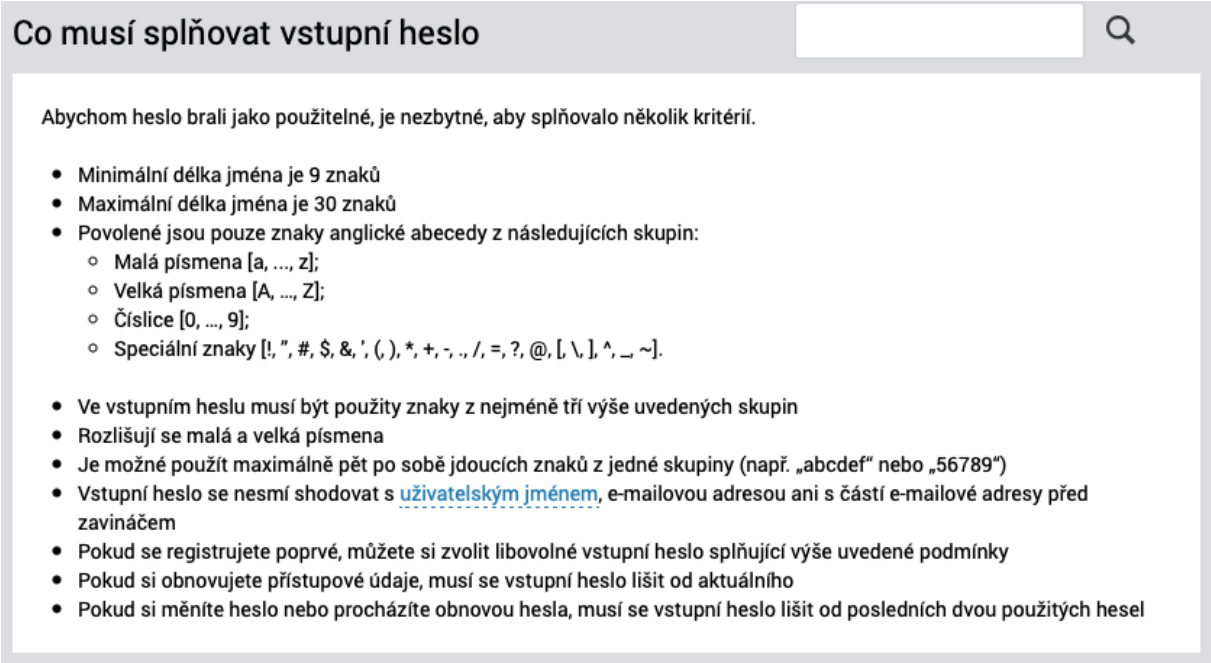
	Č	M	Č+M	Č+M+V	Č+M+V+S
3 znaky	< 1s	< 1s	< 1s	< 1s	< 1s
5 znaků	< 1s	< 2s	< 7 s	1,5 min	< 12 min
10 znaků	< 17 min	< 6 měsíců	< 12 let	2 698 let	192 495 let

Zdroj: Vlastní zpracování

Legenda:

Č = číslo
M = malé písmeno
V = velké písmeno
S = symbol

V dnešní době už mají banky při tvorbě hesla stanovené jisté podmínky, právě z důvodu, aby byla uživateli nastavená hesla dostatečně bezpečná. Příklad takových podmínek je znázorněn na obrázku 2. [26]



Obrázek 2: Tvorba hesla u Poštovní spořitelny

Zdroj: [26]

Takto složitá hesla mohou být pro uživatele těžko zapamatovatelná, hesla by se neměla zapisovat na nezabezpečená místa a ke každému účtu by mělo být heslo jiné, z toho důvodu je pro ulehčení možné používat správce hesel. Správce hesel jsou programy, které v sobě uschovávají hesla, přihlašovací jména nebo čísla platebních karet. Tyto programy většinou umí také generovat nová bezpečná hesla. Další výhodou je, že se hesla nemusí přepisovat, program se připojí k internetovému prohlížeči a navrhne přihlašovací údaje pro tuto stránku. [27]

Speciálním druhem hesla je PIN (Personal Identification Number), který se skládá většinou pouze ze čtyř číslic, proto se může zdát, že je velice jednoduchý na zapamatování, ale ne příliš bezpečný. PIN kód se používá především u platebních karet a mobilních telefonů. Je jednoduchý na zadávání a jeho bezpečnost je podpořena omezeným počtem pokusů. Po několika pokusech se platební karta nebo SIM karta zablokují, buď na určitý časový úsek, např. 5 minut, po uplynutí této doby je možné zkoušet další možnosti PIN kódu, nebo se karta zablokuje způsobem, že na její odblokování je potřeba nějaké jiné heslo. [28]

b) Jednorázové heslo

Jednorázové heslo (one-time password OTP) je automaticky generovaný řetězec numerických nebo alfanumerických znaků, které ověřují uživatele pro jednu transakci nebo jedno přihlášení. OTP může nahradit statické heslo a být použito pro stejné akce, ke kterým se statické heslo používá, nebo může být přidáno jako další bezpečností vrstva. [29]

Jednorázové heslo není snadné k zapamatování, protože se stále mění. Díky tomu je toto heslo bezpečnější. Uživatel si ho nemusí pamatovat. Heslo se automaticky vygeneruje a je uživateli odesláno. Způsobů zasílání OTP je více. Jednou z možností je zaslání přes SMS zprávu, druhou možností je vygenerování tohoto čísla v aplikaci, která je v mobilním telefonu nainstalovaná. Další možností jsou takzvané bezpečnostní tokeny. Bezpečnostní tokeny jsou malá elektronická zařízení, které slouží právě k vygenerování jednorázového hesla, v dnešní době již nejsou bezpečnostní tokeny často využívané, protože jejich funkci nahrazují právě mobilní telefony. Poslední možností pro zaslání OTP je poštou, kdy je vygenerované heslo vytisknuto na papír a zasláno na adresu uživatele. [30]

c) Biometrie

Biometrie pokrývá celou řadu technologií, ve kterých se pro identifikaci a ověřování používají jedinečně identifikovatelné atributy. Mezi ně patří otisky prstů, rozpoznávání obličeje, sken duhovky, hlas, chůze, DNA, tvar ucha, rukopis, způsob psaní na klávesnici a další. [31]

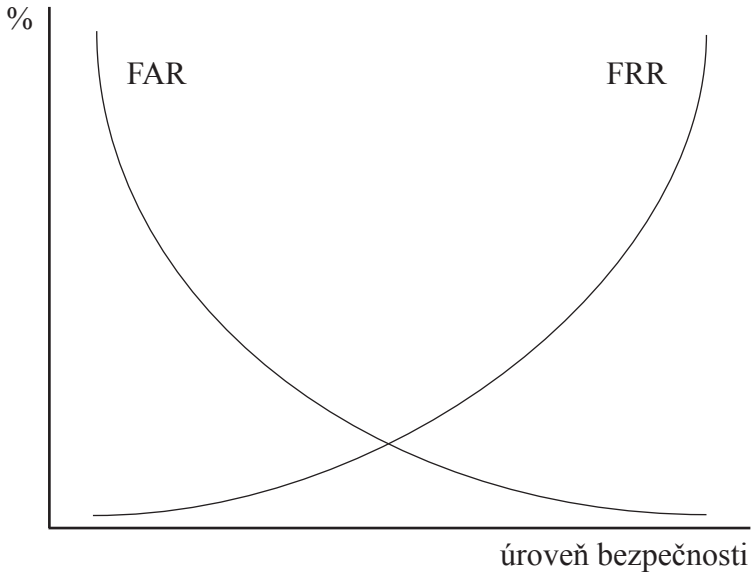
Tyto atributy se dělí do svou skupin [32]:

- Fyziologické vlastnosti jsou většinou přesnější a spolehlivější, protože jsou lépe opakovatelné a nejsou ovlivňovány psychickým a fyzickým stavem, jako je stres nebo nemoc. Mezi fyziologické vlastnosti patří otisk prstu, rozpoznávání obličeje, sken duhovky, DNA, tvar ucha a další.
- Behaviorální vlastnosti jsou méně přesné, protože jsou ovlivňovány psychickým a fyzickým stavem. Jedná se o hlas, chůzi, rukopis, způsob psaní na klávesnici, podpis a další.

Právě z důvodu nepřesnosti se do systému pro ověřování uživatele na základě jeho biometrických vlastností vnáší náhodné a systematické chyby. Výsledky měření především behaviorálních charakteristik jsou proměnné a závisí na faktorech jako je čas, vliv prostředí, fyzický a psychický stav měřené osoby a další. Je téměř jistě, že výsledky dvou měření stejného vzorku nebudou identické. Biometrický systém tedy nemůže ověřit člověka absolutně, ale pouze s určitou pravděpodobností. Tento systém může požadovat stoprocentní shodu, ale v tomto případě by většina uživatelů byla odmítnuta. Aby byl systém použitelný musí v něm být povolena určitá variabilita biometrických charakteristik. Na druhou stranu, čím větší je tato variabilita, tím větší je pravděpodobnost neoprávněného vniknutí. Je-li povolena malá variabilita, jedná se o vysokou bezpečnostní úroveň, v opačném případě nízkou bezpečnostní úroveň. Biometrické systémy se mohou dopustit dvou chyb. [32]

Míra nesprávného přijetí (false acceptance rate – FAR) je měřítkem pravděpodobnosti, že biometrický bezpečnostní systém nesprávně příjme pokus o přístup neoprávněného uživatele. FAR se obvykle udává jako poměr počtu nesprávných přijetí děleno počtem pokusů o identifikaci. [33]

Míra nesprávného odmítnutí (false rejection rate – FRR) je měřítkem pravděpodobnosti, že biometrický bezpečnostní systém nesprávně odmítne pokus o přístup autorizovaného uživatele. FRR je obvykle uváděno jako poměr počtu falešných uznání děleno počtem pokusů o identifikaci. U těchto hodnot platí nepřímá úměra, tzn. čím je větší hodnota FAR, tím je hodnota FRR menší a naopak. Tuto nepřímou úměru můžeme vidět na grafu 3. [33]



Graf 1: Biometrické chyby

Zdroj: upraveno podle [33]

Způsoby rozpoznávání těchto jedinečných vlastností člověka jsou různé. Nejpoužívanější z hlediska dostupnosti je v elektronickém bankovnictví snímání otisků prstu a 3D rozpoznávání obličeje. Tyto dvě možnosti jsou totiž dostupné ve většině nově vyrobených chytrých telefonů. Místo zadávání hesla pak stačí načíst otisk prstu, nebo snímek obličeje. [34]

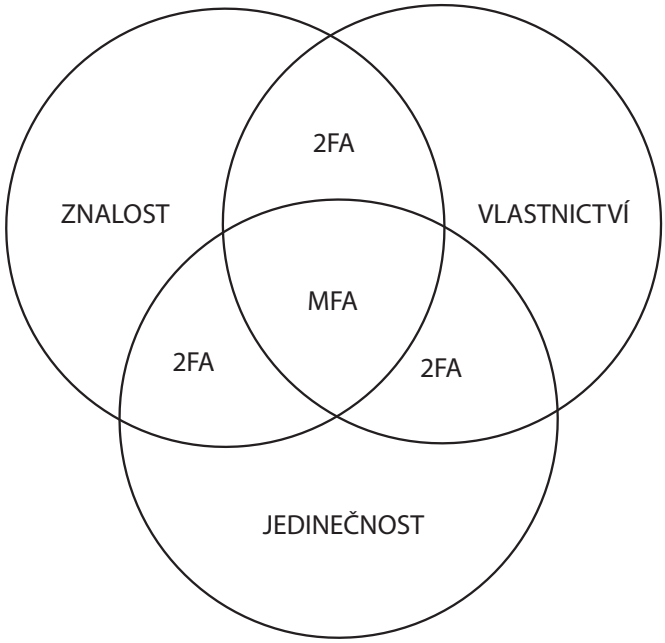
d) Dvoufaktorová a multifaktorová autentizace

Vícefaktorová autentizace (MFA) je autentizační metoda, při které má uživatel přístup pouze po úspěšném předložení dvou nebo více bezpečnostních faktorů. Při použití dvou faktorů se této

autentizaci říká také dvoufaktorová autentizace (2FA). Tyto faktory spadají do tří kategorií [35]:

- znalost – něco, co uživatel zná (např. heslo, PIN kód nebo CVV);
- vlastnictví – něco, co uživatel vlastní (např. jednorázové heslo, chytrý telefon nebo chytré hodinky);
- jedinečnost – něco, čím uživatel je (např. biologické prvky jako je otisk prstu, sken duhovky nebo rozpoznání obličeje);

Prolínání těchto tří kategorií je zobrazeno na grafu 4.



Graf 2: Vymezení 2FA a MFA

Zdroj: upraveno podle [35]

3.2 Bezpečnostní mechanismy internetové stránky

Odposlouchávání přenosů dat na nezabezpečené internetové stránce může být pro útočníky velice jednoduché, proto je důležité, aby webové stránky, na kterých se uživatel rozhodne zadat svoje osobní údaje, byly zabezpečené. Bezpečnost těchto stránek zajišťují mimo jiné certifikáty a protokoly popsané v této kapitole [36]:

a) Public Key Infrastructure (PKI);
b) digitální certifikát;
c) Transport Layer Security (TSL) protokol;

a) Public Key Infrastructure (PKI)

PKI je soubor hardwarových a softwarových prostředků a pracovních postupů, který slouží k bezpečné manipulaci s digitálními certifikáty. PKI zajišťuje generování a distribuci certifikátů od certifikační autority k uživateli, používání certifikátů a jejich zneplatnění. Jinými slovy PKI označuje systém protokolů pro bezpečnou komunikaci v prostředí internetu. [37]

b) Digitální certifikát

Digitální certifikát je elektronický dokument, který je používán k identifikaci jedince, serveru, společnosti nebo jiné entity a ke spojení této identity s veřejným klíčem. Tyto certifikáty vydávají a ověřují certifikační autority (CA). [38]

Certifikát musí obsahovat sériové číslo, datum počátku a konce platnosti, identifikační údaje o subjektu, kterému je certifikát vydán, veřejný klíč a identifikační údaje CA. [39]

Veřejný klíč je jeden ze dvojice klíčů asymetrické šifry. Obě strany, které spolu komunikují, mají veřejný a soukromý šifrovací klíč. Zpráva se posílá společně s veřejným klíčem, rozšifrovat jí může jen majitel veřejného klíče svým soukromým klíčem. [38]

c) Transport Layer Security (TSL) protokol

Předchůdcem TSL protokolu je Secure Socket Layer (SSL) protokol, který se používal k zabezpečení komunikace a přenášených dat mezi prohlížeči a webovými servery. SSL je protokol, který přidá mezi transportní a aplikační vrstvu další vrstvu, která poskytuje zabezpečení komunikace šifrováním a umožní ověření totožnosti komunikujících stran. Protokoly SSL i TSL se využívají pro bezpečnou komunikaci s webovými servery pomocí HTTPS. HTTPS je verze HTTP protokolu, která je zabezpečena právě pomocí TSL protokolu. [38]

4 RIZIKA ELEKTRONICKÉHO BANKOVNICTVÍ

Riziko elektronického bankovnictví je situace, při které za určených definovaných podmínek může dojít ke ztrátě financí klienta, a tím k obohacení útočníka. Útočníkem může být buď jednotlivec nebo, v dnešní době i stále rozšířenějším jevem, celá organizovaná skupina, specializující se právě na prolomení ochranných prvků bank. Proto banky musí neustále vyvíjet nové ochranné prvky a být tak o krok před útočníkem. [40]

4.1 Rizika spojená s používáním internetu

Internet je v dnešní době nejrozšířenějším komunikačním kanálem, kterým protéká nezměrné množství dat. V těchto datech je pro klienta velmi těžké se orientovat, čehož využívají útočníci a pomocí nástrojů níže jmenovaných zneužívají neznalost uživatelů, který nedokáží rozeznat např. útočný e-mail od oficiální e-mailu od banky. [41]

Rizik spojených s používáním internetu je velmi mnoho a stále se objevují nová. V této práci, z důvodu jejího rozsahu, popisuji jen některé z nich:

a) phishing;
b) pharming;
c) malware;
d) sociální inženýrství;

a) Phishing

Phishing je jedním z nejrozšířenějších rizik ve spojení s internetovým bankovnictvím této doby. Slovo phishing vzniklo ze slova fishing, v překladu rybaření, a to z důvodu, že se jedná o podobnou činnost. Útočníci se snaží ulovit přihlašovací údaje, čísla karet a různé další osobní údaje jejich obětí. Definice phishingu podle Jamese (2007 str. 35) znít takto: „Phishing je činnost, kdy je uživateli zaslán padělaný e-mail, který se klamavým způsobem staví do té pozice, že byl odeslán skutečnou finanční institucí ve snaze oklamat příjemce e-mailu tak, aby sdělil své soukromé informace typu čísla platební karty nebo bankovního účtu.“ [42]

První případy phishingu se objevily již roku 1995, ale jako skutečný problém jsou brány od roku 2003, kdy se rozšířily do míry, kdy začali phisheři – útočníci používající phishing, útočit na velké finanční instituce. [43]

Existují různé způsoby, jakými lze phishingový útok provádět. Dnes nejrozšířenější je falešná identita. Další dvě oblíbené metody jsou pak přesměrování a vyskakovací okna. V této práci se budu zabývat převážně falešnou identitou a to proto, že je nejrozšířenější a nejvíce souvisí se samotným internetovým bankovnictvím. Útok metodou falešné identity začíná tím,

že útočník vytvoří velice věrnou kopii webové stránky vstupu do internetového bankovnictví. Kopie se dá vytvořit např. pomocí webového nástroje wget, tento nástroj je určen přímo pro zrcadlení webových stránek. Podoba internetové stránky se díky tomuto nástroji uloží do počítače útočníka, který ji může následně upravit a nahrát na server. Na serveru nastaví, aby odesílal data do anonymní schránky. Anonymní schránka může být buď e-mailový účet nebo jiná internetová stránka, která obsahuje skript ASP nebo PHP, díky čemuž může sbírat data. Aby uživatel nepoznal, že byl oklamán, může útočník na zrcadlené stránce upravit pole pro přihlášení tak, aby se uložily uživatelem uvedené informace a zároveň použít jeho data, aby byl přihlášen do skutečného internetového bankovnictví. Poté už stačí, aby útočník připravil e-mail, který bude obsahovat odkaz na nově vytvořenou internetovou stránku a důvěryhodný text. Do tohoto e-mailu je často přidáváno i logo bankovní společnosti, nebo podpis, aby vypadal přesvědčivěji. Příklad takového e-mailu můžeme vidět na obrázku 3. [42]

Obrázek 3: Příklad podvodného e-mailu

zdroj: [45]

Po obdržení takového e-mailu a kliknutí na odkaz v něm obsažený se dostaneme na stánku, která by mohla vypadat úplně stejně jako opravdová stránka pro přihlášení do internetového bankovnictví. Po vyplnění a odeslání informací se sice uživatel může objevit ve skutečném internetovém bankovnictví své banky, ale kromě toho se však také odešlou jeho přihlašovací údaje útočníkovi do jeho schránky. [44]

Toto je jedna z možností použití této metody, útočníci samozřejmě vytvářejí pořád nové způsoby, ale tato zjednodušená verze, jak by mohl tento útok vypadat, stačí, abychom si mohli představit, jak takový útok funguje. Další metodou je útok přesměrováním. Při útoku přesměrováním útočník vytvoří e-mail, který rovnou obsahuje pole pro zadání důvěrných informací. Po vyplnění se tyto údaje dostanou přímo k útočníkovi. Tento typ se ale používá spíše v elektronických obchodech než v internetovém bankovnictví, proto se s ním nebudu ve své práci nadále zabývat. Poslední metoda se nazývá útok pomocí vyskakovacího okna. Již z jejího názvu vyplývá, že útočník získá informace o uživateli tím, že mu podstrčí falešnou přihlašovací stránku v okamžiku, kdy se chystá vstoupit na stránku pro přihlášení do jeho internetového bankovnictví. Téměř všechny prohlížeče mají v dnešní době zakázaná vyskakovací okna, proto se tato metoda již často nepoužívá. [42]

b) Pharming

Pharming můžeme rozdělit do dvou základních kategorií: globální pharming a lokální pharming. Obě tyto kategorie mají stejný cíl, oklamat uživatele a získat jeho osobní údaje nejen pro přihlášení do internetového bankovnictví. [46]

Globální pharming

Na rozdíl od phishingu, kdy útočník oslovuje přímo koncové uživatele internetového bankovnictví, napadají útočníci DNS server. DNS server je hierarchická databáze, která uchovává internetové domény a jejich příslušné DNS adresy. Zjednodušeně řečeno, každá internetová doména má svou příslušnou IP adresu, která není pro uživatele snadná k zapamatování. DNS server proto tuto IP adresu překládá na příslušnou doménu. Pokud se útočníkovi podaří změnit záznam v tomto serveru, stane se to, že uživatelé připojeni na tento DNS server zadají správnou doménu pro stránku internetového bankovnictví, ale jsou přesměrováni na adresu, kterou se podařilo útočníkovi v DNS serveru pozměnit. Pokud je tato stránka dostatečně věrohodná, je pro běžného uživatele obtížné poznat, že se nachází na falešné stránce. Je proto opravdu důležité kontrolovat certifikát této stránky a obecně všech webových stránek, na kterých se rozhodneme vyplňovat své osobní údaje. [47]

Lokální pharming

Lokální pharming funguje velmi podobně jako globální. Rozdíl je v tom, že útočník nenapadá DNS server, ale konkrétní počítač. V tomto počítači konkrétně soubor hosts, který funguje podobně jako DNS server. Je v něm seznam IP adres a k nim příslušných domén. Pakliže útočník pozmění údaje v tomto souboru, může se stát, že se uživatel opět dostane na falešnou stránku, ze které se dostanou jeho údaje přímo k útočníkovi.

Pharming je mnohem více propracovaná technika než phishing a je mnohem náročnější na provedení. V porovnání s phishingem se proto objevuje velice zřídka. V samotném porovnání dvou druhů pharmingu je více využíván lokální pharming, napadnout DNS server je totiž velmi obtížné, protože je to jedna z nejvíce chráněných částí internetu. [46]

c) Malware

Malware je souhrnné označení pro všechny škodlivé programy, které se snaží napadnout počítač nebo mobilní zařízení. Malware může být používán k poškození nebo ovládnutí systému, ke krádeži dat, k získávání osobních údajů nebo hesel, sledování uživatel a podobně. Nejčastěji se šíří pomocí internetu. Mezi typy malwaru, které mohou být využívány k odcizení údajů týkajících se internetového bankovnictví, patří mimo jiné [48]:

- spyware;
- počítačový virus;
- trojský kůň;
- sniffer;
- typosquatting;

Spyware

Spyware je jeden z typů malwaru. Pomocí spywaru mohou útočníci sbírat informace o chování svých obětí na internetu, má přístup k historii procházení internetu nebo k osobním údajům. Tyto informace může také bez vědomí napadených uživatelů posílat přes internet třetím stranám. Jedním z typů spywaru je keylogger. Tento škodlivý program zaznamenává stisky kláves, čímž se může útočníkovi podařit získat informace jako číslo účtu, platební karty, nebo i uživatelského jména a hesla pro přihlášení do internetového bankovnictví. [49]

Počítačový virus

Počítačový virus je program, který se v počítači může spustit bez vědomí jeho uživatele. Může napadat soubory nebo jiné programy, za účelem jejich zničení, nebo získání z nich dostupných informací. Počítačové viry se nemohou šířit samy, jsou předávány prostřednictvím různých sítí, např. při stahování souborů z internetu, nebo se přenášejí pomocí paměťových médií, jako je DVD, nebo USB disk. [50]

Trojský kůň

Trojský kůň je druh počítačového viru. Podle názvu je patrné, že se vyznačuje tím, že na první pohled vypadá jako užitečný program, který ulehčuje práci, nebo slouží pro pobavení, třeba nějaká hra, ale ve skutečnosti způsobuje škodu. Mimo jiné může právě trojský kůň v souvislosti s pharmingem upravovat soubor host se seznamem domén, provádět v něm změny a nalákat uživatele na falešné stránky, pro získání jeho osobních údajů. [51]

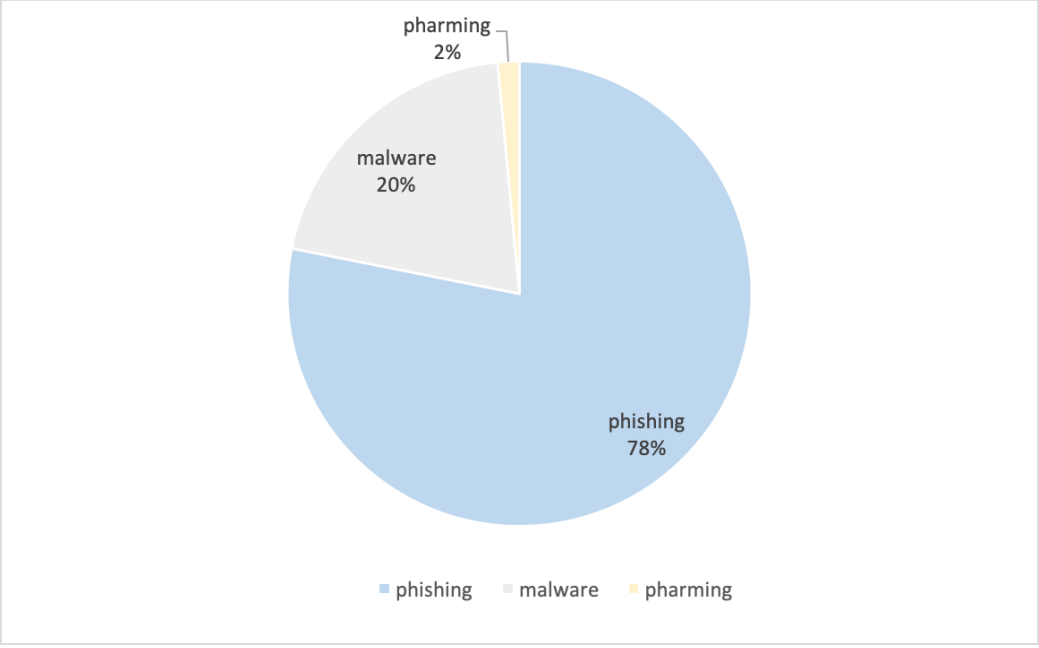
Sniffer

Sniffer je software, který dokáže odposlouchávat, jaká komunikace probíhá na síti Wi-Fi nebo v klasické drátové komunikaci. V případě, že se na této síti nachází někdo, kdo nekomunikuje bezpečně, může útočník odposlouchávat celou tuto komunikaci a dozvědět se jeho osobní informace, čísla kreditních karet nebo hesla. [52]

Typosquatting

Typosquatting využívá překlepů při vyhledávání internetových domén. Uživatel internetu napíše adresu webové stránky, kterou chce navštívit, do svého internetového prohlížeče. Když při tomto úkonu udělá typografickou chybu, může se stát, že se objeví na úplně jiné stránce. Typosquateři tyto stránky využívají ve svůj prospěch. Přetvoří ji tak, aby vypadala stejně jako stránka, kterou chtěl uživatel navštívit, a pokusí se tak ukrást jeho osobní informace nebo heslo k internetovému bankovnictví. [53]

Na grafu 5 je ukázán procentuální výskyt útoků phishing, malware a pharming v roce 2018.



Graf 3: Procentuální výskyt útoků phishing, malware a pharming v roce 2018

zdroj: [54]

d) Sociální inženýrství

Sociální inženýrství je umění manipulace s lidmi, za účelem získání jejich důvěrných informací. Informace, které zločinci hledají jsou různé, mezi nejčastější ovšem patří hesla nebo bankovní informace. Tuto techniku využívají zločinci hlavně z důvodu, že je obyčejně jednodušší oklamat člověka než se nabourat do softwaru. [55]

4.2 Rizika při používání bankomatu

Bankomat se dostal mezi sto nejlepších vynálezů 20. století. Jedná se o automat na výdej peněz. Kromě výdeje peněz je s ním možné provádět i další operace, jako je dotaz na zůstatek na účtu, vkládání peněz a další. Jiným označením pro bankomat je ATM (Automated Teller Machine). Po vložení platební karty do ATM zadá uživatel svůj PIN, čímž prokáže, že je skutečným vlastníkem karty, po úspěšném ověření může provádět operace, které konkrétní bankomat umožňuje. [56]

Rizikům spojeným s používáním bankomatu je věnována tato samostatná kapitola, ve které popisuji již méně časté útoky oproti útokům na internetu. Stále je ale důležité je připomenout. Při používání bankomatu může dojít k odcizení hotovosti, platební karty, PIN kódu nebo údajů obsažených na platební kartě. Mezi rizika při používání bankomatu patří mimo jiné [58]:

- shoulder surfing;
- skryté kamery;
- dotykové senzory;
- skimming;
- card trapping;
- cash trapping;
- falešný bankomat;

Shoulder surfing

Shoulder surfing je metoda, kdy se útočník snaží odpozorovat nahlížením přes rameno PIN kód k platební kartě v době, kdy si jeho oběť vybírá peníze z bankomatu. V případě, že se mu to podaří, pravděpodobně se bude snažit odcizit nebo zkopírovat platební kartu, ke které se mu podařilo PIN kód získat. [57]

Skryté kamery

Skryté kamery jsou většinou používány společně s dalším zařízením, které je nainstalováno na bankomatu. Skrytá kamera má za úkol odpozorovat PIN, který uživatel do bankomatu zadá. Kromě toho může útočník pomocí skryté kamery odpozorovat i číslo karty, datum vypršení její

platnosti a CVV kód, následně pak může tyto údaje využít pro platby na internetu. Skrytá kamera nemusí být nainstalována jen přímo na bankomatu, ale i v jeho blízkosti. [58]

Dotykové senzory

Dotykový senzor bývá umístěn přímo na klávesnici bankomatu. Na rozdíl od skryté kamery, která vizuálně sleduje stisknuté klávesy, mechanismus uvnitř dotykového senzoru zaznamenává úhozy, které uživatel bankomatu provede nevědomě přímo na dotykovém senzoru. Tyto úhozy ovšem skrz dotykový senzor dojdou až na skutečnou klávesnici, díky které jsou prováděny příkazy na bankomatu, proto je velice těžké dotykový senzor odhalit. [58]

Skimming

Útočníci používají skimming ke zkopírování dat, která se nachází na magnetickém proužku platební karty při vložení platební karty do bankomatu. Používají k tomu téměř neviditelné zařízení, které nainstalují přímo před slot pro vložení karty do bankomatu. Při vložení platební karty pak toto zařízení zkopíruje všechny potřebné údaje, přičemž uživatel o tom nemá ani tušení. Tyto údaje pak útočník použije pro vytvoření falešné karty. Aby zkopírovanou platební kartu mohl útočník zneužít, potřebuje znát PIN kód, proto se ve stejné chvíli snaží tento kód odpozorovat metodou shoulder surfing, instalováním nenápadné kamery přímo na bankomat nebo jinými metodami. [59]

Card trapping

Card trapping je podobný skimmingu. V tomto případě útočník nainstaluje na bankomat nenápadné zařízení, které zachytí platební kartu jeho oběti. Ve chvíli, kdy uživatel odejde pro pomoc, nebo svou kartu zanechá v bankomatu z jiného důvodu, kterým může být nabití dojmu, že bankomat zadržel kartu z určitého důvodu, odcizí útočník kartu z předem připravené pasti. I v tomto případě se útočník napřed pokusí odpozorovat PIN jeho oběti. [59]

Cash trapping

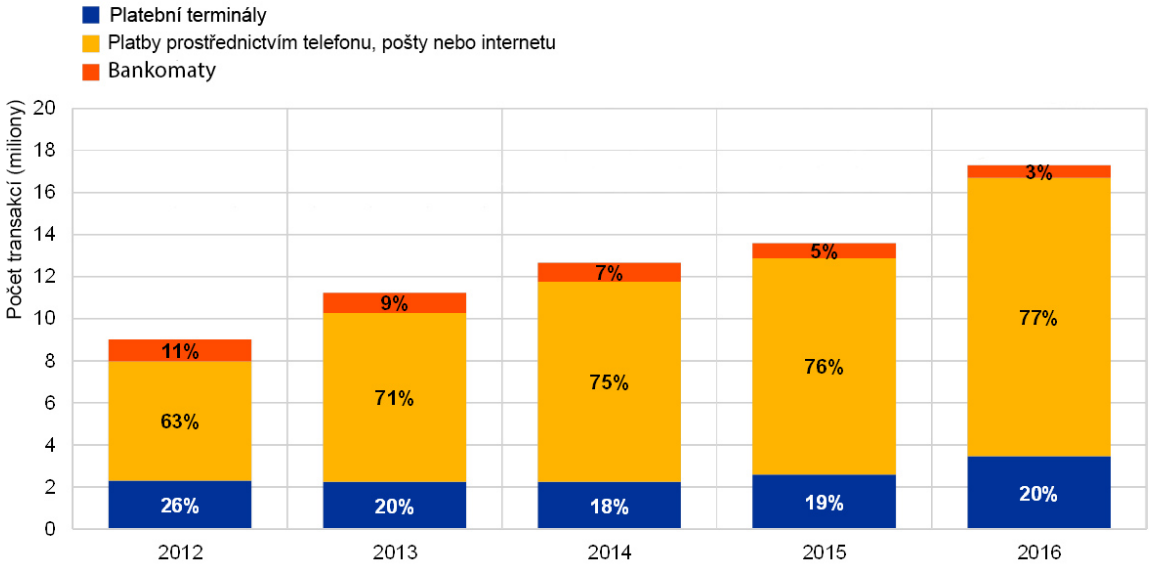
Podobně jako u Card trappingu i tomto případě nainstaluje útočník na bankomat zařízení, které ale tentokrát neslouží k zachycení platební karty, ale k zachycení hotovosti. Když jeho oběť odejde od bankomatu bez své hotovosti, útočník se vrátí a vytáhne zařízení společně s hotovostí, kterou si její skutečný majitel neodnesl. [60]

Falešný bankomat

Falešný bankomat, jak je již z názvu jasné, je napodobenina skutečného bankomatu, kterou vytvořil útočník, za účelem okradení jeho oběti. Falešný bankomat tak může zadržet cizí

platební kartu, přečíst údaje, které se nachází na jejím magnetickém proužku a odpozorovat PIN k této kartě. Falešný bankomat si může útočník upravit podle svých potřeb, je znám případ, kdy ve falešném bankomatu bylo nainstalováno zařízení, které ihned po zadání PIN kódu odeslalo útočníkovi zprávu, která v sobě tento kód obsahovala. [61]

V rámci České republiky nejsou statistiky týkající se zneužití platebních karet zveřejňovány. Na grafu 4 můžeme vidět vývoj celkového počtu podvodů pomocí platebních karet vydaných v rámci SEPA. SEPA je Jednotná oblast pro platby v eurech (Single Euro Payments Area). Zahrnuje 33 evropských států včetně České republiky. [62]



Graf 4: Vývoj celkového počtu podvodů pomocí platebních karet vydaných v rámci SEPA v období 2012 až 2016.

Zdroj: [63]

Z tohoto grafu vyplívá, že nejmenší počet zneužití platební karty je provedeno pomocí bankomatů. Naopak největší počet zneužití je pomocí plateb, při kterých nemusí být platební karta fyzicky přítomna. Tato data jsou z období od roku 2012 až 2016, ale podle rostoucí tendence se dá předpokládat celkový nárůst zneužití platebních karet i v následujících letech. Kromě celkového růstu počtu zneužití platebních karet, roste i zneužití plateb těch, při kterých nemusí být fyzicky přítomna karta. Naopak procent celkového počtu zneužití platební karty u bankomatu postupně ubývá.

5 MINIMALIZACE RIZIK ELEKTRONICKÉHO BANKOVNICTVÍ

V předchozí kapitole jsou popsána nejčastější rizika, která hrozí uživateli elektronického bankovnictví. Jejich odhalení a možnosti jejich minimalizace jsou obsaženy v této kapitole.

5.1 Bezpečné používání platební karty

Platební karty s sebou nesou různá rizika. Jejich zneužití není velmi obtížné, proto je potřeba mít platební kartu pod dohledem. Jednou z možností je nastavení upozornění na pohyby transakcí na kartě prostřednictvím SMS nebo přímo v aplikaci v mobilním telefonu, když pak jedinec, který uživateli ukradne platební karty nebo její údaje provede transakci, je uživatel upozorněn a může tuto kartu nahlásit jako ztracenou nebo odcizenou a zablokovat ji, aby nedošlo k dalšímu neoprávněnému provedení transakce. Když se uživatel z nějakého důvodu rozhodne nepoužívat oznámení o transakcích, je doporučeno kontrolovat průběžně pohyby na účtu prostřednictvím internetového bankovnictví nebo smart bankingu. Dalšími způsoby, jak minimalizovat rizika při používání platební karty může být nastavení limitů na platební kartě, používání platebních karet v mobilním telefonu a další. [64]

LIMITY

Aby se předešlo ztrátě větších částek z účtu, mají platební karty možnost nastavení limitů pro platby a výběr hotovosti.

Pro každou platební kartu je možné nastavit limit pro výběr hotovosti, pro platby kartou v obchodech, pro bezkontaktní platby nebo pro platby na internetu. Tyto limity se liší u každé banky. Doporučené a maximální limity pro tři skupiny podle České spořitelny můžeme vidět v tabulce 3. [65]

Tabulka 3: Doporučené a maximální limity platebních karet

Limity ke kartám		Limity pro výběry hotovosti	Limity pro platby u obchodníků	Limity pro platby na internetu
Karty pro děti 8 až 14 let	Doporučené	2 000	2 000	1 000
	Maximální	50 000	200 000	do výše Vašeho limitu pro platby v obchodech
Karty pro dospělé	Doporučené	20 000	50 000	5 000
	Maximální	50 000	200 000	do výše Vašeho limitu pro platby v obchodech
Prémiové karty	Doporučené	50 000	200 000	10 000
	Maximální	100 000	500 000	do výše Vašeho limitu pro platby v obchodech

zdroj: [65]

Limity si ale může každý upravit podle své potřeby. Pokud např. uživatel nepoužívá platební kartu k placení na internetu, je doporučeno tento limit nastavit na 0 Kč nebo tuto funkci úplně

blokovat. Při způsobech platby, u kterých není potřeba přítomnost karty, je vhodné nastavit limit na nižší částku z důvodu snadnějšího zneužití platební karty tímto způsobem. [66]

PLATEBNÍ KARTY V MOBILNÍM TELEFONU

Placení telefonem je bezpečnější než placení platební kartou z hlediska, že uživatel nemusí vytáhnout skutečnou kartu, na které jsou uvedeny citlivé údaje jako její číslo, datum platnosti a CVV. Kromě mobilních telefonů je možné platby provádět také některými chytrými hodinkami nebo tablety. Možností, jak platit mobilním telefonem je několik. Současně nejvyužívanější služby v České republice jsou [67]:

- aplikace vytvořené bankami;
- Google Pay;
- Apple Pay;

Aplikace vytvořené bankami

Výhodou této kategorie z hlediska bezpečnosti je, že uživatel nemusí poskytovat údaje o své platební kartě nikomu dalšímu než své bance. Vlastní platební aplikaci mají v České republice pouze 3 banky, a to ČSOB, Česká spořitelna a Airbank. Tyto aplikace fungují pouze na telefonech se zařízením Android, které mají funkci NFC. [68]

Google Pay

Služba Google Pay funguje v České republice již od podzimu 2017, funguje na mobilních telefonech s operačním systémem Android a s funkcí NFC. Její fungování zprostředkovává společnost Google. Údaje o platební kartě jsou šifrované uložené na serverech této společnosti. Při používání Google Pay je pro každou platbu vytvořeno virtuální číslo karty, které se odešle obchodníkovi místo skutečného čísla karty. Obchodník pak nemá žádné údaje o tom, kdo provedl tuto platbu. [69]

Apple Pay

Novinou pro Českou republiku v roce 2019 je placení pomocí Apple Pay. Apple Pay je jediná služba, kterou je možné provádět platby pomocí zařízení od Apple. Placení je také prováděno pomocí technologie NFC. Potřebné informace o platební kartě jsou zašifrovány a uloženy na serverech Applu. Jejich dešifrování je možné pouze se zařízením, na kterém je tato karta používána, tzn. že Apple nemá přístup k žádným z těchto informacím. Při placení pomocí Apple Pay je obchodníkovi sděleno specifické číslo zařízení a jedinečný kód transakce. Číslo karty není při transakci předáno, protože toto číslo není uloženo ani na zařízení ani na serverech

Applu. Stejně jako u Google Pay nejsou uschovávány informace, podle kterých by bylo možné spojit uživatele s platbou. [70]

5.1.1 Bezpečné nakupování na internetu

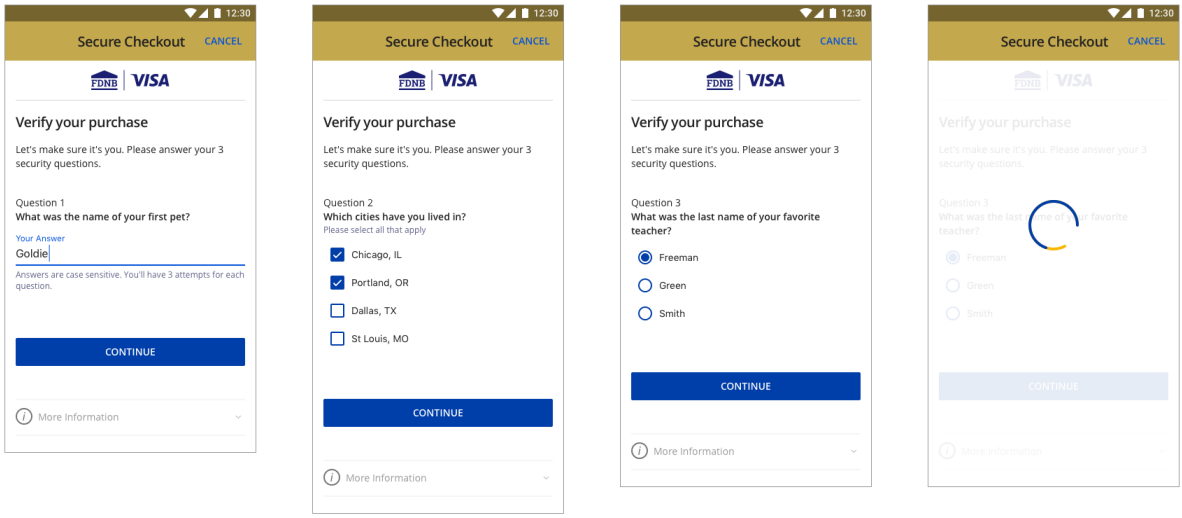
Nakupování přes internet je v dnešní době poměrně běžné, nese však s sebou také různá rizika. Je důležité vybrat spolehlivý e-shop. Můžete objevit e-shop, který nabízí podezřele nízké ceny za zboží. S velkou pravděpodobností tento e-shop nebude bezpečný a je potřeba zkontrolovat, jestli má zabezpečené internetové stránky a prověřit obchodníka. Pokud se jedná o seriózní e-shop, má na svých webových stránkách uvedeny veškeré zákonné údaje jako je obchodní jméno, IČO, DIČ, telefon, adresu a další. Dalším ukazatelem bezpečného e-shopu jsou také recenze od zákazníků. Zvyšovat bezpečnost nakupování na internetu mohou zvyšovat také 3D Secure nebo platební peněženky. [74]

3D SECURE

3D Secure je tří doménový bezpečnostní protokol, jehož cílem je snížení rizik podvodných plateb. Tyto tři domény jsou vydavatel karty, zpracovatelská banka a karetní asociace. Údaje předávané mezi klientem a serverem jsou šifrované a nemůže se k nim dostat žádná třetí osoba včetně obchodníka. 3D Secure je obdobou PIN kódu, který je používán v offline světě. V praxi to znamená, že zákazník po zadání platebních údajů obdrží SMS zprávu s kódem pro potvrzení platby a ověření, že se jedná skutečně o majitele karty, a ne nikoho jiného. [71]

3D Secure přináší výhodu i pro obchodníky. Jeho použitím dojde k přenesení zodpovědnosti, kdyby tedy došlo k podvodu, odpovědnost za škodu pak nenese obchodník, ale vydavatelská brána. [72]

V současné době se pracuje na zavedení 3D Secure 2.0. Vzhledem k posunu technologií a možnosti placení kartou přes mobilní telefon, není zabezpečení z hlediska posílání kódu SMS zprávou dostačující. 3D Secure 2.0. by měl fungovat na principu dvoufaktorové autentizace. K ověření platby pak bude potřeba něco, co uživatel zná, nebo něco, čím uživatel je. Jednou z možností je zavedení ePIN kódu, který by fungoval na stejném principu jako klasický PIN. Uživatel by ho používal ke každému potvrzení platby, další možností je využití biometriky a poslední dosud navrženou možností jsou kontrolní otázky. Na obrázku 4 je ukázka toho, jak by mohl 3D Secure 2.0 vypadat. [71]



Obrázek 4: Secure 2.0

zdroj: [73]

PLATEBNÍ PENĚŽENKY

Jednou z možností placení na internetu je používání platební peněženky. Nejznámější platební peněženkou je PayPal. Do platební peněženky si uživatel nabije kredit buď kartou online, obyčejným převodem, nebo si může propojit s platební peněženkou svou platební kartu. V žádném z těchto případů se při transakci obchodník nedozví údaje o platební kartě. [74]

5.1.2 Bezpečné používání bankomatu

Při výběru z bankomatu je důležité dbát na opatrnost. Prvním krokem je při příchodu k bankomatu bankomat pořádně prohlédnout a ujistit se, že není poničený a že na něm není žádné neobvyklé zařízení. Tato zařízení se obvykle nacházejí u portu na platební kartu nebo u části pro výdej peněz. Nacházet se mohou ale i kdekoliv jinde na bankomatu. [75]

Pro provádění operací, které bankomat umožňuje, je potřeba zadat PIN. Před touto operací je potřeba se ujistit, že nikdo jiný nestojí v diskrétní zóně bankomatu, při zadávání PINu je potřeba dbát zvýšené opatrnosti a zakrýt klávesnici rukou i v případě, že se v blízkosti bankomatu nikdo jiný nenachází. Na bankomatu totiž může být přidělána kamera, která je pro běžného uživatele téměř neviditelná. [76]

Při používání bankomatu dává bankomat jeho uživatelům pokyny. Pro bezpečné použití bankomatu je potřeba dbát na tyto pokyny a neřídit se rady nikoho jiného. Nikdo nemá právo zasahovat do transakci klientů u bankomatu, a to včetně ochranky nebo jiného personálu v bance nebo obchodním centru. [75]

Po provedení transakce vyjede z bankomatu platební karta, vybraná hotovost a v případě, že o ní klient zažádá i stvrzenka. Všechny tyto věci je potřeba ihned uschovat. V případě, že vám bankomat nevydá platební kartu nebo požadovanou hotovost, neodcházejte od bankomatu. Volejte na zákaznickou linku, jejíž telefonní číslo by mělo být na bankomatu uvedeno, nebo se pokuste k sobě přivolat pracovníka banky nebo ochranku. [76]

5.2 Bezpečné používání internetového bankovnictví

K bezpečnému používání internetového bankovnictví je potřeba zvýšené opatrnosti. Nástrahy na jeho uživatele jsou různé. Minimalizovat rizika spojená s jeho používáním je možné různými způsoby. Z důvodu rozsahu této práce jsem vybrala pouze důležitou část z nich:

- aktualizace softwaru;
- antivirus;
- bezpečná Wi-Fi síť;
- rozpoznání podvodných e-mailů;
- bezpečná webová stránka;

AKTUALIZACE SOFTWARU

Aktualizování softwaru je z hlediska bezpečnosti velmi důležité. Aktualizace obsahují opravy chyb, které byly v předchozích verzích, tyto chyby jsou průběžně odhalovány, nejen útočníky, ale i samotnými výrobci softwarů. Chyby jsou výbornou příležitostí pro útočníky, aby do zařízení s neaktualizovaným softwarem nainstalovaly bez vědomí uživatele malware, který může později způsobit velké škody. [77]

ANTIVIRUS

Antivirus je program, který zabraňuje a důsledně eliminuje výskyt škodlivého malwaru v elektronických zařízeních. Takový program by neměl umožnit malwaru, aby se dostal do počítače, nebo jiného zařízení, na kterém je nainstalovaný. Antivirové programy porovnávají data, ve kterých by se mohl skrývat malware a databázi virů, kterou mají k dispozici. [78]

BEZPEČNÁ WI-FI SÍŤ

Veřejně přístupné Wi-Fi sítě nemusí být vždy bezpečné. Útočníci dokáží prostřednictvím monitorování této veřejné sítě sledovat internetovou komunikaci, která na ní probíhá. Když se uživatel rozhodne zadat své přihlašovací údaje na nezabezpečené webové stránce, velice snadno se tyto údaje dostanou k útočníkovi. Webové stránky internetového bankovnictví jsou

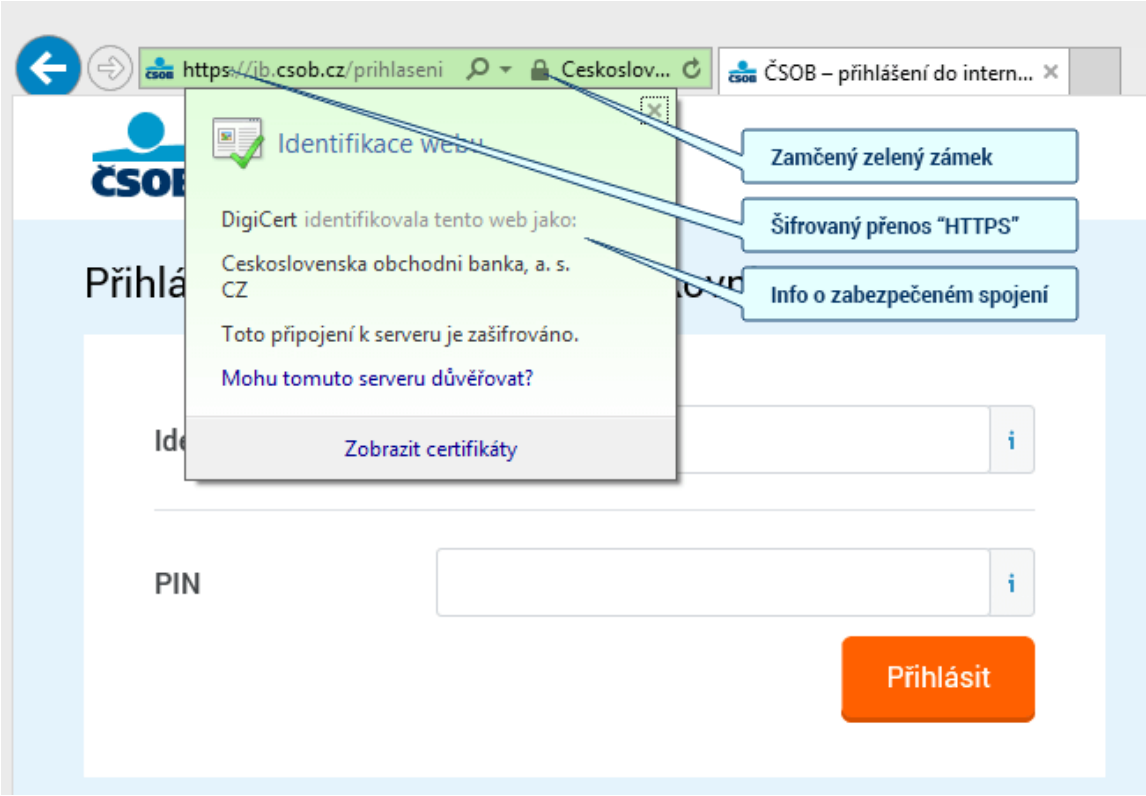
sice zabezpečené, ale spousta uživatelů má jedno heslo k více internetovým účtům a v tomto případě se útočník dostane snadno i do internetového bankovnictví jeho oběti. Je důležité mít pro různé internetové účty různá hesla a snažit se vyhnout používání volně přístupných Wi-Fi sítí. [79]

ROZPOZNÁNÍ PODVODNÝCH E-MAILŮ

Část kapitoly o rizicích elektronického bankovnictví je věnováno podvodným e-mailům, phishingu a pharmingu. Konktrétně phishing podle výzkumů zaujímá první místo podle počtu útoků. Poznat podvodný e-mail je poměrně snadné. Útočníci, kteří tyto e-maily rozesílají, v nich žádají hesla, přihlašovací jména nebo jiné osobní údaje. Banka nikdy zprávy takového typu neposílá. [80]

BEZPEČNÁ WEBOVÁ STRÁNKA

Některé tyto e-maily v sobě obsahují odkaz na webovou stránku, která se na první podle tváří jako přihlašovací stránka do internetového bankovnictví. V adresním řádku této stránky ale pravděpodobně nenaleznete zelený zámek, který v sobě uschovává certifikát o tom, že tato stránka skutečně patří bance. Před vyplněním údajů je potřeba ověřit, jestli se jedná o podvodnou stránku nebo ne. Na obrázku 5 můžeme vidět, že v adresním řádku se nachází HTTPS a zámek, po jehož rozkliknutí vidíme, že doména patří Československé obchodní bance. [81]



Obrázek 5: Zabezpečená webová stránka pro vstup do internetového bankovnictví

Zdroj: [81]

Ověřovat, jestli se jedná o podvodnou stránku, nebo ne, nestačí pouze po otevření odkazu, který přišel e-mailem. Kontrolovat přihlašovací webovou stránku je důležité pokaždé, kdy se rozhodnete vyplnit své osobní údaje. Ať už se jedná o internetové bankovnictví, e-shop nebo jakoukoliv jinou webovou stránku. Odkazy v podvodném e-mailu by se v žádném případě neměly otevírat, samotný vstup na podvodnou internetovou stránku může být nebezpečný. [81]

V případě, že obdržíte podezřelý e-mail, nebo navštívíte podezřelou webovou stránku pro vstup do internetového bankovnictví vždy kontaktujte vaši banku a tuto událost nahlaste. [82]

5.3 Bezpečné používání smart bankingu

Chytré telefony, na kterých si uživatel může nainstalovat smart banking se dají používat velice podobně jako počítače, proto je při používání smart bankingu potřeba dodržovat stejnou opatrnost jako u internetového bankovnictví. Oproti počítači však mobilní telefony přinášejí i jiné možnosti minimalizace rizik např. instalováním vhodné aplikace nebo zámkem telefonu. [83]

INSTALOVÁNÍ APLIKACE

Rozdíl mezi internetovým bankovnictvím a smart bankingem je ten, že internetové bankovnictví je přístupné přímo v internetovém prohlížeči, kdežto smart banking potřebuje

ke svému fungování aplikaci. Obdobně pak s internetovým bankovnictvím, kdy by si měl uživatel ověřit, jestli se nachází na opravdových stránkách internetového bankovnictví, měl by si při instalaci aplikace pro používání smart bankingu ověřit, zda si stahuje správnou aplikaci, vydanou jeho bankou. [83]

Nejen aplikace smart bankingu, ale i jakékoliv jiné aplikace, které si uživatel instaluje do svého zařízení je doporučeno stahovat pouze z oficiálního obchodu s aplikacemi jako je Google Play pro Android nebo App Store pro Apple. Bohužel ani stahování aplikací z těchto oficiálních obchodů není stoprocentně bezpečné, proto je potřeba před stáhnutím jakékoliv aplikace zkontrolovat, jestli je od důvěryhodného vydavatele. Ukazatelem, jestli se jedná o bezpečnou aplikaci, mohou být i její recenze. [82]

Při nainstalování aplikace do chytrého telefonu lze nastavit, k čemu bude mít aplikace v telefonu přístup. Pro zvýšení bezpečnosti by měla mít aplikace povolený přístup pouze k věcem, které skutečně potřebuje. [83]

ZÁMEK TELEFONU

Mobilní telefon je zařízení, které většinou nosíme u sebe, čímž se zvyšuje pravděpodobnost jeho ztráty nebo odcizení. Nastavením hesla nebo jiného bezpečnostního prvku pro vstup do zařízení se výrazně snižuje riziko, že se neoprávněná osoba dostane k osobním údajům majitele mobilního telefonu. [84]

ZÁVĚR

Elektronické bankovnictví nám v mnohém ulehčuje každodenní život. Ať se jedná o používání platebních karet, nakupování přes internet nebo kontrolování zůstatku na účtu pomocí smart bankingu. Všechna tato ulehčení však s sebou přináší i rizika.

Cílem této bakalářské práce bylo pospat vybraná z těchto rizik a nalézt možnosti, jak se dají minimalizovat.

K uvedení do problému elektronického bankovnictví byla v první kapitole přiblížena jeho historie, konkrétně vznik elektronického bankovnictví ve světě a jeho začátky v České republice. Pro popsání rizik elektronického bankovnictví je potřeba zjistit, jaké druhy existují, tomuto tématu je věnována druhá kapitola, kde jsou jednotlivé druhy blíže popsány. Třetí kapitola je věnována bezpečnostním mechanismům, které zabezpečují elektronické bankovnictví. Tyto mechanismy jsou rozděleny do dvou podkapitol. Na bezpečnostní mechanismy pro ověření uživatele, kde se jedná například o heslo, biometrii a další. Druhou podkapitolou jsou bezpečnostní mechanismy internetových stránek. Následující kapitola v sobě obsahuje nejrozšířenější rizika dnešního elektronického bankovnictví a poslední kapitola je věnována možnostem, jak tato rizika odhalit a minimalizovat.

Vzhledem k tomu, že neexistuje žádná souhrnná statistika zahrnující, jak rizika spojená s platebními kartami, tak rizika spojená s používáním internetu, rozhodla jsem se závěrečné shrnutí výsledku této práce rozdělit na dvě skupiny. První skupina jsou rizika spojená s používáním internetu. Tato rizika a jejich opatření jsou znázorněny v tabulce 4.

Tabulka 4: Rizika a opatření pro používání elektronického bankovnictví prostřednictvím internetu

riziko	pravděpodobnost nastání rizika	opatření
phishing	1	Rozpoznávání podvodných e-mailů
		Rozpoznání bezpečné webová stránky
		Používání Antiviru
pharming	3	Rozpoznání bezpečné webová stránky
		Používání Antiviru
malware	2	Používání Antiviru
		Bezpečná síť Wi-Fi
		Aktualizace softwaru
		Způsob instalování aplikace
		Zámek telefonu

Zdroj: vlastní tvorba

Tato tabulka obsahuje tři nejčastěji se vyskytující rizika spojená s používáním elektronického bankovnictví prostřednictvím internetu. Pravděpodobnost nastání rizika je ve stupnici od jedné do tří, kde jedna znamená největší pravděpodobnost, že dané riziko nastane.

Z této tabulky jsem následně vytvořila seznam opatření podle jejich důležitosti sestupně. Tento seznam je vidět v tabulce 5.

Tabulka 5: Seznam opatření při používání elektronického bankovnictví prostřednictvím internetu seřazený podle důležitosti sestupně

Rozpoznávání podvodných e-mailů
Rozpoznání bezpečné webová stránky
Používání Antiviru
Bezpečná síť Wi-Fi
Aktualizace softwaru
Způsob instalování aplikace
Zámek telefonu

Zdroj: vlastní tvorba

Stejným způsobem je popsána druhá skupina, která v sobě zahrnuje rizika spojená s používáním platební karty. Přehledová tabulka této skupiny je zobrazena v tabulce 6.

Tabulka 6: Rizika a opatření spojená s používáním platební karty

riziko zneužití platební karty	pravděpodobnost nastání rizika	opatření
u platebního terminálu	2	limity pro čerpání peněz z účtu
		platební karty v mobilním telefonu
prostřednictvím telefonu, pošty nebo internetu	1	limity pro čerpání peněz z účtu
		3D Secure
		Platební peněženky
u bankomatu	3	limity pro čerpání peněz z účtu
		Bezpečné používání bankomatu

Zdroj: vlastní tvorba

I z této tablky jsem následně vytvořila seznam opatření podle jejich důležitosti sestupně. Tento seznam je vidět v tabulce 7.

Tabulka 7: Seznam opatření spojených s používáním platební karty seřazený podle důležitosti sestupně

limity pro čerpání peněz z účtu
3D Secure
Platební peněženky
limity pro čerpání peněz z účtu
platební karty v mobilním telefonu
Bezpečné používání bankomatu

Zdroj: vlastní tvorba

V těchto tabulkách jsou shrnuta vybraná rizika elektronického bankovnictví a možnosti jejich minimalizace. Dále pak seřazení opatření rizik podle důležitosti. Tato důležitost vyplívá z pravděpodobností nastání jednotlivých rizik. Je ale důležité podotknout, že by se všechna tato opatření měla alespoň zvážit. V ideálním případě pak provést. Čím více těchto opatření uživatel provede, tím budou finance na jeho účtu ve větším bezpečí.

Většina informačních zdrojů, ze kterých jsem v této práci čerpala, jsou zdroje na internetu. A to především z důvodu jejich aktuálnosti. Elektronické bankovnictví se stále vyvíjí a stále se objevují nová rizika i možnosti zabezpečení, která ještě v tištěných dokumentech nejsou obsažená.

Přínosem této práce je přiblížení elektronického bankovnictví jejím čtenářům. Čtenář se v této práci seznámí s riziky, která se při používání elektronického bankovnictví mohou objevit a dozví se, jak se chovat, aby tato rizika minimalizoval. Snažila jsem se tuto práci psát tak, aby byla srozumitelná pro uživatele na všech úrovních znalostí elektronického bankovnictví.

POUŽITÁ LITERATURA

[1] PLISCHKE, Simona Ely. Jak došly platební karty do českých zemí: aneb historie karet plná zajímavostí. Peníze.cz [online]. 27. 4. 2007 [cit. 2019-04-23]. Dostupné z: https://www.penize.cz/platebni-karty/18777-jak-dosly-platebni-karty-do-ceskych-zemi-aneb-historie-karet-plna-zajimavosti

[2] JUŘÍK, Pavel. Platební karty: ilustrovaná historie placení. Praha: Libri, 2012. ISBN 978-80-7277-498-2.

[3] Včera novinka, dnes samozřejmost. Jak internetové bankovnictví změnilo svět financí. C Journal [online]. 19. 4. 2018 [cit. 2019-04-23]. Dostupné z: https://www.c-journal.cz/clanky/jak-internetove-bankovnictvi-zmenilo-svet-financi/

[4] Rozvoj bezhotovostních forem placení. Česká národní banka [online]. [cit. 2019-04-23]. Dostupné z: https://www.historie.cnb.cz/cs/bezhotovostni_platebni_styk/pruzerova_temata_bezhotovostni_platebni_styk/rozvoj_bezhotovostnich_forem_placeni.html

[5] Výzkum pro ČBA: Kvalita elektronického bankovnictví je pro Čechy zásadní [online]. 7. 6. 2018 [cit. 2019-04-23]. Dostupné z: https://scac.cz/nas-vyzkum-pro-cba-kvalita-elektronickeho-bankovnictvi-je-pro-cechy-zasadni-tretina-by-kvuli-nemu-i-zmenila-banku/

[6] VESELÍKOVÁ, Monika. Placení bez hotovosti. Kartou, nálepkou i mobilem. Peníze.cz [online]. 24. 10. 2017 [cit. 2019-04-24]. Dostupné z: https://www.penize.cz/ucty-karty/327543-placeni-bez-hotovosti-kartou-nalepkou-i-mobilem

[7] PŘÁDKA, Michal. Elektronické bankovnictví: rady a tipy. Praha: Computer Press, 2000. Praxe manažera (Computer Press). ISBN 80-722-6328-5.

[8] Bezhotovostní peníze, platební prostředky. Proč se finančně vzdělávat [online]. 6. 5. 2016 [cit. 2019-04-23]. Dostupné z: https://www.psfv.cz/cs/penize-a-ucty/bezhotovostni-penize

[9] MORAVEC, Ondřej. Nejasnosti kolem čipových karet [online]. 16. 3. 2006 [cit. 2019-04-23]. Dostupné z: https://archiv.ihned.cz/c1-22896395-nejasnosti-kolem-cipovych-karet

[10] Co to je CVV/CVC a kde se nachází? [online]. [cit. 2019-04-23]. Dostupné z: https://help.gopay.com/cs/tema/bezpecnost/co-to-je-cvv-cvc-a-kde-se-nachazi

[11] Platební karty a jejich druhy [online]. [cit. 2019-04-23]. Dostupné z: https://www.penize.cz/15744-platebni-karty-a-jejich-druhy

[12] Near Field Communication Credit Cards[online]. 1 March 2019 [cit. 2019-04-23]. Dostupné z: https://www.finder.com.au/nfc-credit-cards

[13] Bezkontaktní karta Mastercard. Mastercard [online]. [cit. 2019-04-23]. Dostupné z: https://www.mastercard.cz/cs-cz/zakaznici/sluzby-technologie-benefity/platebni-sluzby/contactless.html

[14] Souhrnné statistiky NFC. Sdružení pro bankovní karty [online]. [cit. 2019-04-23]. Dostupné z: http://www.bankovnikarty.cz/pages/czech/profil_statistiky.html

[15] CHVÁTAL, Dalibor Z. Apple Pay, Google Pay, Garmin Pay, Fitbit Pay. S jakými kartami fungují?. Měšec [online]. 25. 2. 2019 [cit. 2019-04-23]. Dostupné z: https://www.mesec.cz/clanky/apple-pay-google-pay-garmin-pay-fitbit-pay-s-jakymi-kartami-funguji/

[16] Homebanking (domácí bankovnictví). Měšec [online]. [cit. 2019-04-23]. Dostupné z: https://www.mesec.cz/financni-portal/ucty/homebanking-domaci-bankovnictvi/

[17] Home banking. Peníze.cz [online]. 14. 7. 2003 [cit. 2019-04-23]. Dostupné z: https://www.penize.cz/investice/15651-home-banking

[18] Internetové bankovnictví. Měšec [online]. [cit. 2019-04-23]. Dostupné z: https://www.mesec.cz/financni-portal/ucty/internetove-bankovnictvi/

[19] CO TO JE INTERNETBANKING A JAK FUNGUJE?. Bezpečně online[online]. [cit. 2019-04-23]. Dostupné z: https://bezpecne-online.saferinternet.cz/surfuj-bezpecne/internetbanking/item/151-co-to-je-internetbanking-a-jak-funguje

[20] Smart banking: vaše finance vždy po ruce. UniCredit Bank [online]. [cit. 2019-04-23]. Dostupné z: https://www.unicreditbank.cz/cs/obcane/digital/smart-banking.html

[21] Přímé bankovnictví. Finance [online]. [cit. 2019-04-23]. Dostupné z: https://www.finance.cz/ucty-a-sporeni/bezne-ucty/abeceda-beznych-uctu/prime-bankovnictvi/

[22] Bezpečnostní mechanismy. Vaše bezpečnost, naše informace [online]. [cit. 2019-04-23]. Dostupné z: http://vasebezpecnost.osobni-stranka.cz/nova-stranka-202184/

[23] Silné ověření klienta podle RTS. Epravo[online]. 3. 4. 2017 [cit. 2019-04-23]. Dostupné z: https://www.epravo.cz/top/clanky/silne-overeni-klienta-podle-rts-ke-smernici-psd2-105724.html

[24] Vytvoření silného hesla a zabezpečení účtu. Google[online]. [cit. 2019-04-23]. Dostupné z: https://support.google.com/accounts/answer/32040?hl=cs

[25] Bezpečnost hesla. Matematika [online]. [cit. 2019-04-23]. Dostupné z: https://matematika.cz/bezpecnost-hesla

[26] Co musí splňovat vstupní heslo. Poštovní spořitelna [online]. [cit. 2019-04-23]. Dostupné z: https://ib.postovnisporitelna.cz/web/ps-napoveda/nastaveni/muj-profil/co-musi-splnovat-vstupni-heslo

[27] EMPEY, Charlotte. Jak si vybrat nejlepší správce hesel. Avast [online]. 30. 12. 2018 [cit. 2019-04-23]. Dostupné z: https://blog.avast.com/cs/jak-si-vybrat-nejlepsi-spravce-hesel

[28] Přihlašování pomocí PINu. Je čas [online]. 21. 12. 2016 [cit. 2019-04-23]. Dostupné z: http://jecas.cz/pin

[29] ROUSE, Margaret. One-time password: OTP. Search Security [online]. listopad 2018 [cit. 2019-04-23]. Dostupné z: https://searchsecurity.techtarget.com/definition/one-time-password-OTP

[30] WOODFORD, Chris. Two-factor authentication. Explain that stuff [online]. October 13, 2018 [cit. 2019-04-23]. Dostupné z: https://www.explainthatstuff.com/how-security-tokens-work.html

[31] What is Biometrics?. Biometrics Institute[online]. [cit. 2019-04-23]. Dostupné z: https://www.biometricsinstitute.org/what-is-biometrics/

[32] MATYÁŠ, Vašek a Jan KRHOVJÁK. Autorizace elektronických transakcí a autentizace dat i uživatelů. Brno: Masarykova univerzita, 2008. ISBN 978-80-210-4556-9.

[33] THAKKAR, Danny. False Acceptance Rate (FAR) and False Recognition Rate (FRR) in Biometrics. Bayometric [online]. [cit. 2019-04-23]. Dostupné z: https://www.bayometric.com/false-acceptance-rate-far-false-recognition-rate-frr/

[34] GOTTWALD, Matěj. Rozpoznání obličeje, nebo otisk prstu?. Lenovo [online]. 8. 3. 2018 [cit. 2019-04-24]. Dostupné z: http://www.lenovoblog.cz/2018/03/rozpoznani-obliceje-nebo-otisk-prstu.html

[35] EISELT, Zbyněk. CO ZNAMENÁ SILNÉ OVĚŘENÍ KLIENTA (SCA) A PROČ SE O NĚM VŠUDE MLUVÍ?. GoPay [online]. 7. 3. 2019 [cit. 2019-04-23]. Dostupné z:

https://www.gopay.com/blog/co-znamena-silne-overeni-klienta-sca-a-proc-se-o-nem-vsude-mluvi/

[36] 7 klíčových rad v zabezpečení webových stránek. IT network [online]. [cit. 2019-04-24]. Dostupné z: https://www.itnetwork.cz/programovani/nezarazene/pr-clanky/7-klicovych-rad-v-zabezpeceni-webovych-stranek

[37] Základní pojmy zabezpečení. Západočeská univerzita v Plzni [online]. [cit. 2019-04-23]. Dostupné z: https://support.zcu.cz/index.php/Základn%C3%AD_pojmy_zabezpečen%C3%AD

[38] SSL CERTIFIKÁTY PRO WWW STRÁNKY. SSL mentor [online]. [cit. 2019-04-23]. Dostupné z: https://www.sslmentor.cz/ssl/ssl-certifikaty

[39] Certifikáty a jejich použití. Bezpečně online [online]. [cit. 2019-04-23]. Dostupné z: http://www.szrcr.cz/uploads/spravci_AIS/Certifika_ty_a_jejich_pouz_iti_v1_17.pdf

[40] MEČÍŘOVÁ, Lucie. Kdy jsou vaše peníze na internetbanking v ohrožení?. Finance[online]. 27. 7. 2017 [cit. 2019-04-24]. Dostupné z: https://www.finance.cz/494805-rizika-ib/

[41] Nebezpečí na internetu, aneb jak vyzrát na rizika online světa. Porovnej 24 [online]. 1. 11. 2018 [cit. 2019-04-24]. Dostupné z: https://www.porovnej24.cz/nebezpeci-internetu-aneb-vyzrat-rizika-online-sveta

[42] JAMES, Lance. Phishing bez záhad. Praha: Grada, 2007. ISBN 80-247-1766-2.

[43] Co je phishing. Antimalware [online]. [cit. 2019-04-24]. Dostupné z: https://www.antimalware.cz/blog/co-je-phishing

[44] Co je phishing?. Avast [online]. [cit. 2019-04-24]. Dostupné z: https://www.avast.com/cs-cz/c-phishing

[45] Scam e-mails – phishing. Koba [online]. 3. 6. 2015 [cit. 2019-04-24]. Dostupné z: https://www.koba.sk/security/current-threats/scam-e-mails-phishing-6.shtml

[46] BEDNÁŘ, Vojtěch. Pharming je zpět a silnější. Lupa [online]. 23. 3. 2007 [cit. 2019-04-24]. Dostupné z: https://www.lupa.cz/clanky/pharming-je-zpet-a-silnejsi/

[47] What is Pharming & How to Prevent it?. Kaspersky [online]. [cit. 2019-04-24]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/pharming

[48] Malware. Avast [online]. [cit. 2019-04-24]. Dostupné z: https://www.avast.com/cs-cz/c-malware

[49] Spyware. Avast [online]. [cit. 2019-04-24]. Dostupné z: https://www.avast.com/cs-cz/c-spyware

[50] Počítačový virus. Avast [online]. [cit. 2019-04-24]. Dostupné z: https://www.avast.com/cs-cz/c-computer-virus

[51] Trojský kůň. Avast [online]. [cit. 2019-04-24]. Dostupné z: https://www.avast.com/cs-cz/c-trojan

[52] Co je to WiFi/Packet Sniffer a kde si ho můžu opatřit a co bych o tom měl vědět?. 365 tipu [online]. 3. 10. 2015 [cit. 2019-04-24]. Dostupné z: https://365tipu.cz/2015/10/03/tip276-co-je-to-wifipacket-sniffer-a-kde-si-ho-muzu-opatrit-a-co-bych-o-tom-mel-vedet/

[53] What is Typosquatting?. McAfee [online]. 3. 7. 2013 [cit. 2019-04-24]. Dostupné z: https://securingtomorrow.mcafee.com/consumer/family-safety/what-is-typosquatting/

[54] Statistiky řešených incidentů. CSIRT[online]. [cit. 2019-04-24]. Dostupné z: https://www.csirt.cz/page/2635/statistiky-resenych-incidentu/

[55] What is Social Engineering?. Webroot [online]. [cit. 2019-04-24]. Dostupné z: https://www.webroot.com/au/en/resources/tips-articles/what-is-social-engineering

[56] Bankomat. Peníze.cz [online]. [cit. 2019-04-24]. Dostupné z: https://www.penize.cz/interaktivni-grafiky/242908-bankomat

[57] Shoulder Surfing. Safe Internetbanking [online]. [cit. 2019-04-24]. Dostupné z: https://www.safeinternetbanking.be/en/fraud-techniques/shoulder-surfing

[58] Taking a Trip to the ATM?. FBI [online]. 14. 7. 2011 [cit. 2019-04-24]. Dostupné z: https://www.fbi.gov/news/stories/atm-skimming

[59] Skimming and card trapping. Safe internet banking [online]. [cit. 2019-04-24]. Dostupné z: https://www.safeinternetbanking.be/en/fraud-techniques/skimming-and-card-trapping

[60] CashTapping. Bezpečné banky [online]. [cit. 2019-04-24]. Dostupné z: https://www.bezpecnebanky.cz/cashtrapping

[61] The Biggest Skimmers of All: Fake ATMs. Krebs on security [online]. 13. 12. 2013 [cit. 2019-04-24]. Dostupné z: https://krebsonsecurity.com/2013/12/the-biggest-skimmers-of-all-fake-atms/

[62] SEPA countries. European central bank [online]. [cit. 2019-04-24]. Dostupné z: https://www.ecb.europa.eu/paym/retpaym/paymint/sepa/html/index.en.html

[63] Executive summary [online]. [cit. 2019-04-24]. Dostupné z: https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport201809.en.html#toc11

[64] Jak bezpečně používat platební kartu. Česká spořitelna [online]. [cit. 2019-04-24]. Dostupné z: https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/bezpecnostni-desatero-platebni-karta

[65] Doporučené a maximální limity k platebním kartám České spořitelny. Česká spořitelna [online]. 1. 9. 2018 [cit. 2019-04-24]. Dostupné z: https://www.csas.cz/static_internet/cs/Komunikace/Interni_komunikace/Informacni_kniha/Prilohy/1_2_PK_Limity.pdf

[66] Zneužili mi platební kartu. Měšec [online]. [cit. 2019-04-24]. Dostupné z: https://www.mesec.cz/financni-portal/ucty/zneuzili-mi-platebni-kartu/

[67] Placení mobilem pro začátečníky. Air Bank[online]. 4. 4. 2018 [cit. 2019-04-24]. Dostupné z: https://www.airbank.cz/novinky/placeni-mobilem-pro-zacatecniky

[68] CVEJNOVÁ, Veronika. Jaké banky umožňují placení telefonem pomocí NFC?. DUO finance [online]. 18. 10. 2018 [cit. 2019-04-24]. Dostupné z: https://www.duofinance.cz/banky-placeni-mobilem-nfc

[69] Google pay. Google pay [online]. [cit. 2019-04-24]. Dostupné z: https://pay.google.com/about/

[70] Podpora pro Apple Pay. Apple [online]. [cit. 2019-04-24]. Dostupné z: https://support.apple.com/cs-cz/apple-pay

[71] HAMBALÍKOVÁ, Karin. JAKOU ZMĚNU V PLACENÍ PŘINESE 3D SECURE 2.0?. GoPay[online]. 19. 3. 2019 [cit. 2019-04-24]. Dostupné z: https://www.gopay.com/blog/jakou-zmenu-v-placeni-prinese-3d-secure-2-0/

[72] What is the 3D Secure liability shift, and when does it occur?. Adyen[online]. [cit. 2019-04-24]. Dostupné z: https://support.adyen.com/hc/en-us/articles/115001766824-What-is-the-3D-Secure-liability-shift-and-when-does-it-occur-

[73] Visa 3DS 2.0 User Experience Guidelines. Visa [online]. [cit. 2019-04-24]. Dostupné z: https://developer.visa.com/pages/visa-3d-secure

[74] Jak bezpečně platit na internetu. D test[online]. 17. 4. 2018 [cit. 2019-04-24]. Dostupné z: https://www.dtest.cz/clanek-6607/jak-bezpecne-platit-na-internetu

[75] Návod na výběr peněz z bankomatu v ČR i v zahraničí. Půjčka [online]. 14. 3. 2018 [cit. 2019-04-24]. Dostupné z: https://www.pujcka.co/navod-na-vyber-penez-z-bankomatu-v-cr-i-v-zahranici

[76] Jak vybrat hotovost z bankomatu?. Finanční portál [online]. [cit. 2019-04-24]. Dostupné z: http://financni-portal.cz/jak-vybrat-hotovost-z-bankomatu

[77] Bezpečné internetové bankovnictví: Je váš internetový prohlížeč opravdu bezpečný?. C journal [online]. 28. 3. 2018 [cit. 2019-04-24]. Dostupné z: https://www.c-journal.cz/clanky/bezpecne-internetove-bankovnictvi-je-vas-internetovy-prohlizec-opravdu-bezpecny/

[78] Co je antivir. Správa sítě [online]. [cit. 2019-04-24]. Dostupné z: https://www.sprava-site.eu/antivir/

[79] Jak je to s bezpečností veřejných Wi-Fi?. Újezd [online]. 27. 8. 2018 [cit. 2019-04-24]. Dostupné z: https://www.ujezd.net/bezpecnost-verejne-wifi

[80] Upozornění na podvodné e-maily. Fio banka [online]. 10. 8. 2015 [cit. 2019-04-24]. Dostupné z: https://www.fio.cz/spolecnost-fio/media/aktuality/166641-upozorneni-na-podvodne-e-maily

[81] Zásady bezpečného užívání elektronického bankovnictví. ČSOB [online]. [cit. 2019-04-24]. Dostupné z: https://www.csob.cz/portal/bezpecnost/jak-se-branit/zasady-bezpecneho-uzivani-elektronickeho-bankovnictvi

[82] Jak chránit své internetové bankovnictví. Česká spořitelna [online]. [cit. 2019-04-24]. Dostupné z: https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/bezpecnostni-desatero-internetove-bankovnictvi

[83] ONDRÁČKOVÁ, Kamila. Nepodceňujte zásady bezpečnosti smartbankingu. Pozor na aplikace i hesla. FinExpert [online]. 26. října 2018 [cit. 2019-04-24]. Dostupné z: https://www.e15.cz/finexpert/setrime/nepodcenujte-zasady-bezpecnosti-smartbankingu-pozor-na-aplikace-i-hesla-1352841

[84] Zásady bezpečného užívání služby Era smartbanking. Poštovní spořitelna[online]. [cit. 2019-04-24]. Dostupné z: https://www.postovnisporitelna.cz/portal/documents/2664281/3651019/SB-zasady.pdf/