Krádež identity

Bc. Pavel Hubáček

Diplomová práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Pavel Hubáček**
Osobní číslo:	**A12344**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Krádež identity**
Téma anglicky:	**Identity Theft**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na dané téma.**
2. **Proveďte analýzu problematiky, spojené s fenoménem krádež identity.**
3. **Definujte způsoby zneužití nabyté identity.**
4. **Možnosti ochrany proti zcizení identity.**
5. **Proveďte návrh a způsoby realizace ochrany osobní identity.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **HARRIS, Shon, Allen HARPER, Chris EAGLE, Jonathan NESS a Michael LESTER. Manuál hackera. Praha: Grada, 2008. ISBN 978-80247-1346-5.**
2. **JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha: Grada, 2007. ISBN 978-80-247-1561-2.**
3. **LANCE, James, Lubomír DLOUHÝ. Phishing bez záhad. Praha: Grada, 2007. ISBN 80-247-1766-2.**
4. **POŽÁR, Josef. Manažerská informatika. Plzeň: Vydavatelství Aleš Čeněk, 2010. ISBN 978-80-7380-276-9.**
5. **RAK, Roman. Biometrie a identita člověka ve forenzních a komerčních aplikacích. 1. vyd. Praha: Grada, 2008. ISBN 978-80-247-2365-5.**

Vedoucí diplomové práce: **PhDr. Mgr. Stanislav Zelinka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **7. února 2014**

Termín odevzdání diplomové práce: **27. května 2014**

Ve Zlíně dne 7. února 2014

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tato diplomová práce se zabývá problematikou krádeže identity. Cílem je identifikovat příčiny vzniku krádeží a navrhnout ochranná opatření proti nim. Teoretická část popisuje možné způsoby identifikace osob pomocí fyzických dokladů a následně se věnuje identifikátorům používaným ve virtuálním prostředí. Praktická část se zaměřuje na aktuální metody krádeže a zneužití identity, dále na využívaná bezpečností opatření. V závěru jsou navržena doporučení sloužící k eliminaci rizik těchto krádeží.

Klíčová slova:

Krádež identity, osobní doklady, identifikace, bezpečnost.

ABSTRACT

This master thesis deals with the problem of identity theft. The aim is to identify the causes of thefts and propose protective measures against them. The theoretical part describes possible ways of identifying people by physical evidence and then it concentrates on identifiers used in a virtual environment. The practical part focuses on current methods of identity theft and misuse, followed by using safety measures. In the conclusion, there are proposed recommendations used for eliminate the risks of these thefts.

Keywords:

Identity theft, personal documents, identification, security

Na tomto místě bych rád poděkoval vedoucímu diplomové práce panu PhDr. Mgr. Stanislavu Zelinkovi za jeho ochotu, trpělivost a věcné připomínky, které dopomohly k vypracování práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl jsem seznámen s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

S krádeží identity se setkáváme již od nepaměti. V současné době se změnila pouze její podoba. Místo fyzického vydávání se za jinou osobu, ať již na základě ukradených listin, či pouhým zevnějškem, jsme dnes uváděni v omyl na základě prostředků počítačové komunikace. Oběťmi mohou být bankovní ústavy, velké nadnárodní korporace, známé osobnosti, ale i prostí občané. Je třeba si uvědomit, že téma krádeží identit se stal globálním problémem, který má základnu především ve Spojených státech.

Cílem diplomové práce je popsat identifikační prostředky, kterými se osoby prokazují ve styku s okolním světem, definovat jejich slabá místa a doporučit opatření k jejich eliminaci.

Práce je rozdělena na část teoretickou a praktickou. V teoretické části jsem přiblížil problematiku daného tématu, pro přehlednost opřenou o diagram struktury práce. Následující část je věnována identifikačním prostředkům z oblasti sociální identity, mezi které nejčastěji řadíme osobní doklady. Druhý způsob, kterým můžeme prokázat svoji totožnost, jsem zařadil do oblasti virtuální identity, Zde se jedná především o problematiku, jakou se jednotlivé osoby prezentují v prostředí internetu. Jde tedy především o rodná čísla, emailové adresy, účty pro různé webové stránky a jiné. Závěr teoretické části je věnován legislativě a výběru zákonů, které s danou problematikou úzce souvisí.

V praktické části jsou charakterizovány možnosti a metody zneužití identity, ke kterým jsou přiřazeny způsoby ochrany, jak preventivní tak technickou formou. Mnoho konkrétních metod páchání této trestné činnosti, které jsou dnes známé, jsou pro pachatele dostatečně bezpečné. Nejsilnějším impulzem v rozvoji této trestné činnosti se stal internet. Slouží ke komunikaci, kooperaci a k obchodům pachatelů. Organizovaný zločin, který vznikl v tomto odvětví, stále roste. Existují organizované skupiny nebo jednotlivci obchodující s citlivými informacemi. Tito lidé využívají techniky anonymního prostředí internetu.

V závěru práce jsou prezentovány návrhy a postupy pro bezpečné nakládání s identitou při vystupování v každodenním životě tak při vystupování v prostředí internetu.

I. TEORETICKÁ ČÁST

1 ÚVOD DO PROBLEMATIKY

Technologický vývoj a nové způsoby komunikace s ním spojené podstatně ovlivnily většinu oblastí moderního života. Tradiční způsoby komunikace mezi lidmi, organizacemi a institucemi se mění, jsou doplňovány a zčásti i nahrazovány novými formami, umožněnými rozvojem elektronické komunikace, internetu, e-mailového spojení apod. Nelze považovat za překvapující, že na tyto nové možnosti komunikace reagují také pachatelé trestné činnosti, kteří je nejen využívají jako operativní a hůře zachytitelný způsob spojení, ale jejich prostřednictvím napadají a neoprávněně využívají, resp. zneužívají uložené nebo sdělované dokumenty, data, informace atd. V důsledku toho i trestné činy natolik klasické a tradiční, jako jsou krádež a podvod, mohou nabývat nových forem páchání.

Spáchání podvodu, při kterém se pachatel vydává za někoho jiného, není žádnou zbrusu novou formou kriminality. Zvláštním, respektive novým se stává, využívá-li moderních komunikačních struktur našeho současného světa, páchá-li se jejich prostřednictvím a odehrává se v jejich prostředí. Jsme stále více propojeni prostřednictvím komunikačních technologií, které slouží nejen ke sdělování informací v elektronické podobě, ale také k jejich vytváření a uchovávání. Masové rozšiřování informačních, komunikačních a sociálních sítí umožňuje v podstatě v kterémkoli okamžiku propojení subjektů na lokální i globální úrovni.

Naše identita byla dříve potvrzována listinnými dokumenty, vandrovní knížkou, glejtem, rodným listem, cestovním pasem, občanským průkazem, řidičským průkazem, a jinými průkazy a legitimacemi, jejichž součástí posléze často bylo i zobrazení podoby držitele.

Nyní, ve virtuálním světě počítačů, serverů, sítí, databází, elektronicky sdělovaných a sdílených informací nevystupujeme ani osobně, ani prostřednictvím fyzických dokladů, ale také „jen“ virtuálně. Naše identita může být vyjadřována a určována kódy, PINy, hesly, které nám umožňují přístup k našim účtům, k naší poště, opravňují nás k nakládání s našimi či firemními prostředky, umožňují použití mobilního telefonu, vstup do databází k údajům, které v nich uchováváme atd.

Zatímco jsme dříve drželi své listinné identifikační doklady tak říkajíc v ruce a jejich ztrátu či zcizení jsme v relativně krátké době snadno zaznamenali, jsou nyní naše identifikační údaje ve virtuálním světě databází a sítí jaksi vedle nás a mimo nás. K jejich zneužití v tom

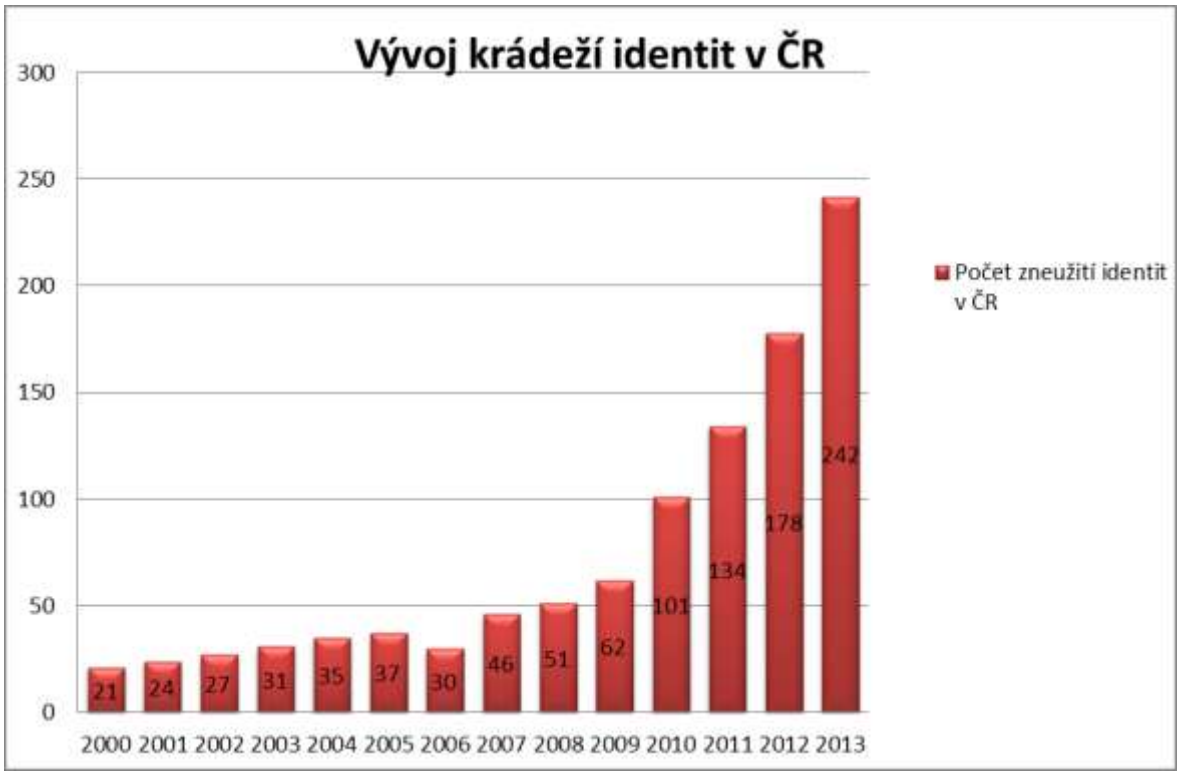
smyslu, že by nám zcela zmizely, v podstatě nedochází (pokud nejsou nějakým zásahem zničeny, resp. vymazány; pak se ale obvykle nejedná o „krádež“, ale o poškození nebo zničení), a proto jejich zneužití většinou zjišťujeme, až když shledáme, že jsme byli nějakým způsobem poškozeni my, nebo s použitím našich identifikačních údajů někdo jiný.

Stále větší závislost společnosti na informačních a komunikačních systémech tak zvyšuje naši zranitelnost kriminalitou, zasahující tyto systémy. Krádež a zneužití cizí identity proto nepředstavuje ve své podstatě nový jev, ale jev, který nabyl některých nových forem vázaných na moderní informační systémy, který se v současných podmínkách rychle šíří, působí značné škody a je předmětem intenzivní diskuse. [1]

1.1 Situace v ČR

Ze statistik je zřejmé, že krádeže identity nabírají rostoucí tendenci. Navíc se dozvíme jen o zlomku faktických útoků. Protiprávních aktivit na internetu je mnohem více avšak dle vyjádření PČR k dané problematice se jich stovky vyřeší jen upozorněním přímo na internetové síti, domluvou či včasným upozorněním. Množit se ale začínají i kauzy, které skončí až u soudu. Nejčastěji jde o mezilidské „vyřizování účtů“ či snahu obohatit se na cizí účet.

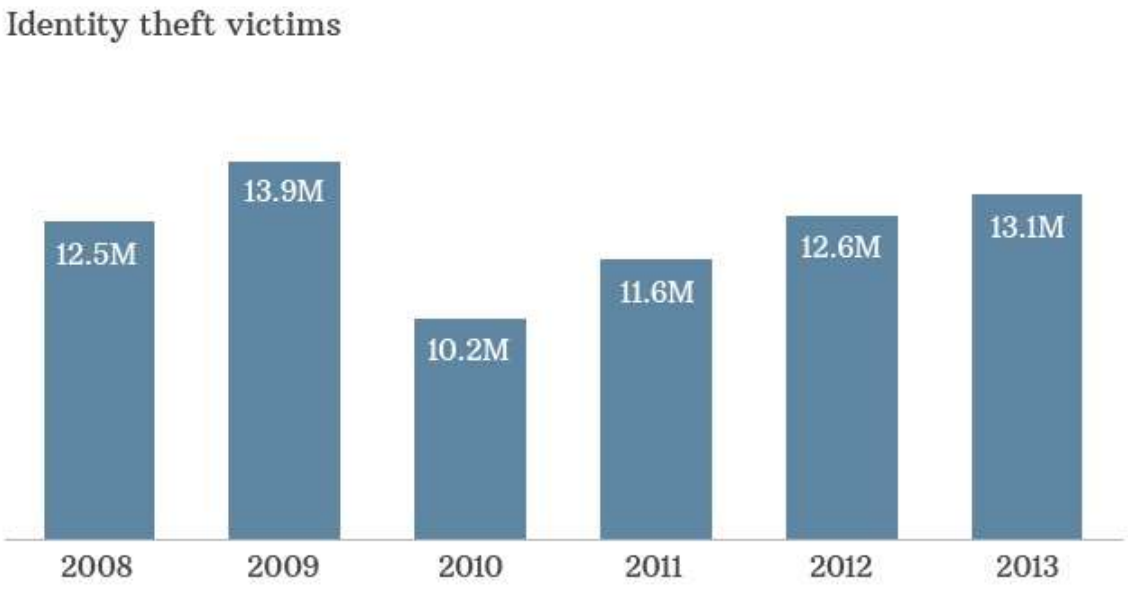
Z níže uvedených statistik vyplývá, že detektivové řešili v roce 2000 jen ojedinělé případy zneužití soukromých hesel a údajů ve virtuálním prostoru, přesně 21. V roce 2009 už jich strážci zákona evidovali 62. A za loňský rok ještě bezmála třikrát více – 242.



Obrázek 1 Vývoj krádeží identit v ČR [2]

1.2 Situace v zahraničí

V USA a státech západní Evropy má v s problematikou krádeže identity zkušenost každý desátý člověk, což tento trestný čin řadí mezi jeden z nejrychleji rostoucích zločinů. Podle národního průzkumu společnosti FTC (Federal Trade Commission), bylo za loňský rok hlášeno cca 13,1 mil. stížností osob, které se staly obětí tohoto podvodného jednání, což tvoří 7% všech obyvatel USA ve věku nad 16 let. Náklady s přímými i nepřímými ztrátami z krádeží identity se odhadují v celkové výši 24,7 miliard dolarů.



Obrázek 2 Vývoj krádeží identit v USA [3]

2 KRÁDEŽ IDENTITY

Jde o podvodné jednání, kdy se někdo vydává za druhého člověka, s cílem získat finanční prostředky, důležité informace nebo jiné výhody, řadíme pod pojem Identity Theft, čili krádež identity nebo totožnosti.

Dostanou-li se osobní údaje do nepovolaných rukou, může podvedená osoba velmi rychle přijít nejen o peníze na svém účtu, ale může nastat i situace, kdy se musí zodpovídat za nezaplacené výdaje, za různé škody, dokonce i nést důsledky mnoha trestných činů, které sice spáchala cizí osoba, ale jejím jménem. Dokazovat skutečnost, že ten, kdo vše způsobil a spáchal, jsem nebyl já, není ani trochu jednoduché.

Zcizení identity může mít několik podob a může být provedeno více způsoby:

Největší nebezpečí představuje finanční krádež identity, kdy podvodník zneužije citlivé osobní údaje oběti pro přístup k bankovnímu účtu, kreditní kartě a má možnost si tak pronajmout v půjčovnách auta, která zpětně už nevrátí, nakupovat zbraně, objednávat si hotelové pokoje a za své služby neplatit, uzavírat různé smlouvy apod.

- kriminální krádež identity, kdy se pachatel vydává za jinou osobu a orgánům činným v trestním řízení poskytne místo vlastních údajů, údaje odcizené.
- krádež identity za účelem vytvořit si zcela novou identitu a začít život jinde jako nový člověk.

Za citlivé informace, které by mohly podvodníky zajímat, můžeme považovat nejen jméno a příjmení, rodná čísla a čísla osobních dokladů, ale veškeré údaje, podle kterých je možno osobu určit, tedy i čísla, PIN a bezpečnostní kódy kreditních karet, adresa bydliště, rodinné či pracovní poměry, detaily o hypotékách a úvěrech apod.

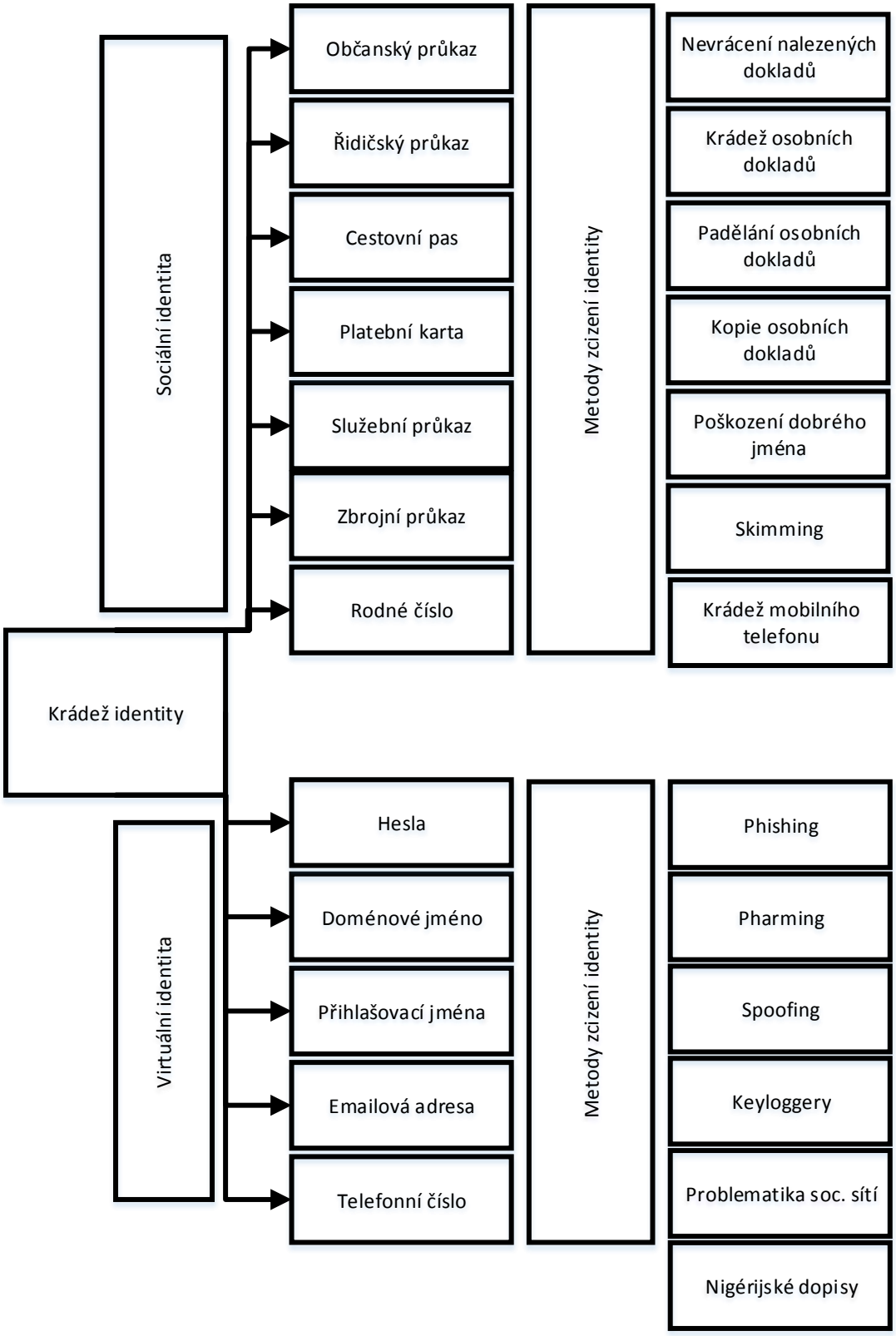
Z hlediska krádeže osobních věcí, jako je batoh, kabelka, kufr, jejichž obsahem je zpravidla peněženka s řidičským průkazem, pasem, platební kartou trvá poškozené osobě detekovat svoji ztrátu a učinit příslušná opatření k eliminaci škod.

Pokud ale údaje pachatel nepozorovaně zkopíruje či odpozoruje, mohou být zneužity a doba, po kterou může pachatel po nabitou identitu figurovat, se výrazně navýší (např. rodné číslo – citlivý identifikační znak každé osoby, který dnes používá mnoho institucí od nemocnic, pojišťoven, bank aj.). A právě touto skutečností, převážně spojenou s vidinou finančního prospěchu si potencionální zločinec může zjistit různorodé, pro něj často velmi

zajímavé a lákavé informace typu: jaká je Vaše finanční situace, kolik vlastníte nemovitostí, kde pracujete, jaký je Váš zdravotní stav apod.

Dnes se poměrně často setkáváme s útoky na platební karty nebo kódy PIN, právě od nich mají podvodníci k přímému zisku nejblíže. Organizované skupiny podvodníků mohou instalovat na peněžité bankomaty např. čtecí zařízení s miniaturním kamerovým systémem, který načte údaje z magnetického proužku či odpozoruje kód PIN. Častý způsob, jak podvodníci mohou uškodit je instalace plastového obdélníčku se smyčkou, který kartu přímo zachytí a již ji zpět nevydá.

Na druhou stranu je potřeba však upozornit na skutečnost, že ne všechny informace, které jsou pro nás citlivé, jsou získávány podvodem. Mnozí lidé dobrovolně a bez zaváhání vyplňují různé osobní formuláře, registrační dotazníky, soutěže, marketingové průzkumy a s využitím svých údajů souhlasí. Při vyplňování různých dotazníků proto zvažujte jakékoliv poskytování citlivých osobních údajů. [18]



Obrázek 3 Struktura práce

3 VYMEZENÍ KLÍČOVÝCH POJMŮ

V kapitole jsou uvedeny základní pojmy z oblasti bezpečnosti v informačních systémech, které velmi úzce souvisí s problematikou práce.

3.1 Elektronický podpis

Jde podpis v takové formě, která, zpravidla kryptografickými metodami, zaručuje integritu dokumentu a autentizaci podepsaného. Pro některé účely je navíc vyžadován zaručený elektronický podpis pouze s předepsanými typy certifikace, tedy založený na kvalifikovaném certifikátu. Zaručený elektronický podpis dokumentu zajišťuje:

- autenticitu – lze ověřit původnost (identitu subjektu, kterému patří elektronický podpis)
- integritu – lze prokázat, že po podepsání nedošlo k žádné změně, soubor není úmyslně či neúmyslně poškozen
- nepopiratelnost – autor nemůže tvrdit, že podepsaný elektronický dokument nevytvořil (tzn. nemůže se zříct své identity)
- může obsahovat časové razítko, které prokazuje datum a čas podepsání dokumentu

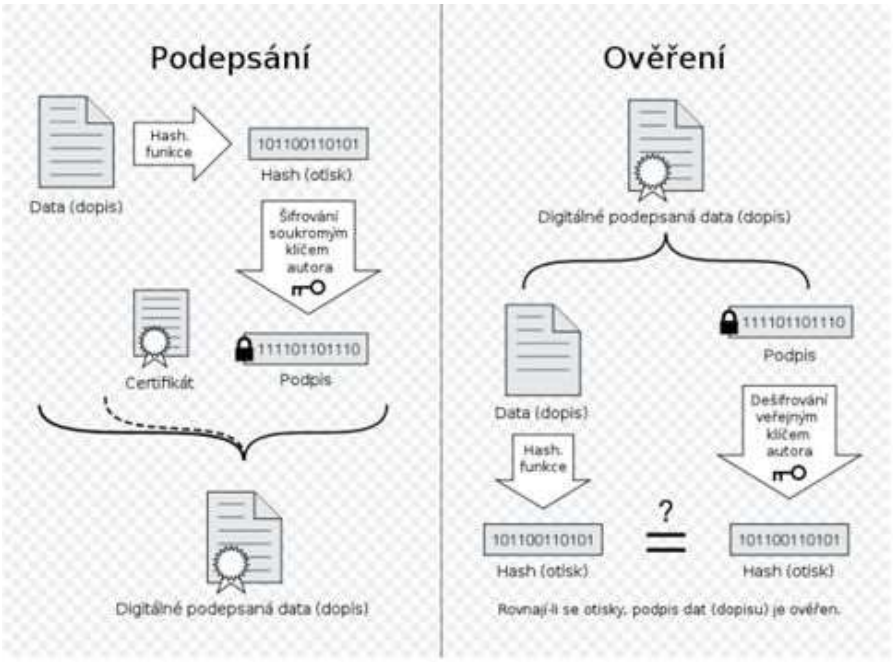
Za elektronický podpis se v širším významu považuje i prosté nešifrované uvedení identifikačních údajů (například jména a adresy, názvu a sídla, rodného nebo jiného identifikačního čísla atd.) na konci textu v elektronické (digitální) podobě, které zaručuje identifikaci (tedy jednoznačné určení) označené osoby, avšak nikoliv integritu podepsaného dokumentu ani autentizaci podepsaného.

Zaručený elektronický podpis je aplikací asymetrické kryptografie (tj. kryptografie s veřejným klíčem). Výjimečně může k jeho vytvoření posloužit i symetrická kryptografie, pak jde ovšem o arbitrovaný protokol. Principem běžného elektronického podpisu je tedy zašifrování dokumentu tajným klíčem a jeho následné dešifrování veřejným klíčem.

Z praktických důvodů se místo celého dokumentu šifruje pouze jeho hash - což je jakási digitální obdoba otisku prstů. Při vytváření hashe pro šifrovací účely se používají takové algoritmy, že je prakticky vyloučené změnit dokument takovým způsobem, aby se současně nezměnil jeho hash. Algoritmy pro vytvoření elektronického podpisu jsou:

- Asymetrické kryptovací algoritmy s veřejným klíčem, nejčastěji RSA (Rivest-Shamir - Adleman) a DSA (Digital Signature Algorithm)
- Bezpečné kryptografické jednocestné algoritmy (hašovací funkce), nejčastěji MD5 (Message Digest 5) spolu s RSA a SHA (Secure Hash Algorithm) spolu s DSA

Ověření podpisu pak spočívá v dešifrování hashe (podpisu) pomocí veřejného klíče autora, nezávislého výpočtu hashe z dokumentu a porovnání obou hodnot. Pokud si odpovídají, pak je podpis ověřen a dokument je považován za důvěryhodný. [3,5]



Obrázek 4 Elektronický podpis [3]

Elektronický podpis vydávají tzv. certifikační autority, které byly akreditovány Ministerstvem vnitra.

3.2 Digitální serverové certifikáty

Komerční certifikáty pro servery jsou určené pro bezpečnou komunikaci serverů. Jsou vydávány pro fyzické nebo právnické osoby na základě řádně vytvořené žádosti o certifikát. Platnost certifikátu je vždy časově omezena. Ověřují a hlavně zaručují, že server se kterým komunikujete je skutečně server např. banky pro internetové bankovnictví, školní server, internetový obchod atp. Serverový certifikát tedy slouží pro zabezpečenou komunikaci internetového prohlížeče se serverem pomocí protokolu SSL (Secure Socket Layer). Poslední verze internetových prohlížečů nápadněji zvýrazňují stupeň důvěryhodnosti právě prohlíženého webového serveru při šifrovaném spojení protokolem HTTPS. Okénko adresního řádku je doplněno o ikonu zamčeného visacího zámku, což indikuje, že je spojení šifrováno pomocí SSL, a přibylo tlačítko identifikace webového serveru, které informuje o jeho provozovateli a také o autoritě, která jej prověřila. [6]

Obrázek 5 HTTPS Česká spořitelna [7]

3.3 Autorizace třetí stranou

Ověřující stranou je typicky banka, která buď zamítne, nebo potvrdí transakci použitím bezpečného venkovního kanálu (např. pošta, telefon). Typické použití je u objednávek po telefonu či mailu. Typické použití je u plateb typu CNP (Cardholder not present), dříve

zvané MO / TO (Mail order / Telephone order). Kdokoliv, kdo zná data z kreditní karty, může vyvolat transakci a odpovědný uživatel pak musí toto potvrdit nebo naopak říci, že jde o nepovolenou transakci. [6]

3.3.1 Heslo

Transakce chráněná heslem požaduje, aby každá zpráva od autorizované strany zahrnovala šifrovanou část pro kontrolu. Tato část je vypočítána pomocí tajného klíče, který je znám pouze autorizující a ověřující straně.

3.4 Další pojmy

Krádež (zcizení) identity (identity theft) - trestný čin vydávání se za někoho jiného s pomocí jeho soukromých informací za účelem finančního či jiného zisku. Mezi nejčastější příklady patří úvěrové podvody s využitím odcizených osobních dokladů.

Zneužití identity – neoprávněné konání pod cizí identitou. Nebezpečí zneužití identity spočívá ve škodě vůči třetím osobám a škodě vůči vlastníkovi předstírané identity

Identita – totožnost, či jednoznačné určení jedinečného subjektu.

Identifikace - jednoznačné určení fyzické osoby ve smyslu datového odlišení od jiných osob

Osobní údaj - jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.

Citlivý údaj - osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a jakýkoliv biometrický nebo genetický údaj subjektu údajů. [8]

4 SOCIÁLNÍ IDENTITA A PROSTŘEDKY IDENTIFIKACE

Sociální identita je charakterizována daty, která lze osobě přiřadit i bez použití IT, např. jméno, adresa, datum narození, občanský průkaz, pas, rodný list. Jde tedy o technické prostředky či listinné dokumenty, ke kterým se mnohdy v rámci informačních systémů přiřazují další soubory, a to např.:

- přihlašovací jméno/heslo u webové aplikace se zadáním jména a adresy
- e-mailová adresa
- telefonní číslo
- osobní číslo v zaměstnání
- doménové jméno
- PINY

4.1 Občanský průkaz

Občanský průkaz je veřejná listina, kterou občan prokazuje své jméno, popřípadě jména, příjmení, rodné číslo, podobu, státní občanství České republiky, jakož i další údaje v ní zapsané. Dále může obsahovat záznamy uvedené na žádost držitele, jako akademický titul a vědeckou hodnost, údaje o manželovi nebo partnerovi, údaje o nezletilých dětech. Podoba držitele průkazu se prokazuje portrétní fotografií, která musí splňovat zákonem stanovená kritéria a musí odpovídat současné podobě držitele. Podobizna je na občanském průkazu spolu s vlastnoručním podpisem digitálně zpracovaná. Občanský průkaz je vydáván s omezenou dobou platnosti stanovenou zákonem. Jeho držitel je povinen v případě pozbytí jeho platnosti zažádat o vydání nového průkazu u patřičného úřadu.

V případě ztráty jakéhokoliv osobního dokladu je jeho držitel povinen neodkladně tuto skutečnost ohlásit příslušnému správnímu úřadu. V případě ztráty občanského průkazu je občanovi vydáno potvrzení o občanském průkazu s uvedením jména, příjmení, rodného čísla, adresy trvalého bydliště a dalších osobních údajů včetně čísla původního občanského průkazu. Smyslem tohoto dokladu je dočasná náhrada občanského průkazu v situacích, kdy je osoba vyzvána k prokázání své totožnosti do doby vydání nového občanského průkazu, o nějž musí občan požádat nejpozději ve lhůtě patnácti dní. Příslušný úřad zároveň zajistí, aby byl nahlášený ztracený nebo odcizený občanský průkaz neplatný a to jeho zanesením

do celostátní databáze neplatných dokladů, kterou spravuje Ministerstvo vnitra České republiky a tuto databázi zpřístupňuje na svých internetových stránkách jako službu pro veřejnost za účelem prevence zneužití ztracených a odcizených dokladů. Rozhodné je v tomto případě datum oznámení takové skutečnosti, před tímto datem může nést jeho držitel následky z neoznámení ztráty nebo odcizení. [9,11]

Obrázek 6 Občanský průkaz ČR [10]

4.2 Cestovní pas

Cestovní pas je veřejná listina opravňující občana k překročení hranic České republiky, nestanoví-li jinak mezinárodní smlouva, jíž je Česká republika vázána. Cestovním dokladem občan prokazuje své jméno, popřípadě jména, příjmení, rodné číslo, podobu, státní občanství České republiky a další údaje zapsané nebo zpracované v cestovním dokladu. Cestovní pas může obsahovat i nosič dat s biometrickými údaji fyzické osoby, pomocí kterých je usnadněna identifikace předkladatele cestovního dokladu jako oprávněného držitele. Cestovní doklady vedle umožnění vstupu na cizí území rovněž deklarují držiteli právo na ochranu v zahraničí státem, který dokument vydal. [9]

4.3 Řidičský průkaz

Řidičský průkaz České republiky a mezinárodní řidičský průkaz vydaný Českou republikou mají status veřejné listiny, z toho důvodu je lze považovat za dokumenty prokazující totožnost jejich oprávněného držitele. Vydávání řidičských průkazů je upraveno Zákonem č. 31/2001 Sb., o řidičských průkazech a registrech řidičů. Současně požadovaný formát řidičského průkazu musí obsahovat vedle stupně oprávnění k řízení motorového vozidla také jméno, popřípadě jména, příjmení, datum a místo narození, rodné číslo držitele, datum

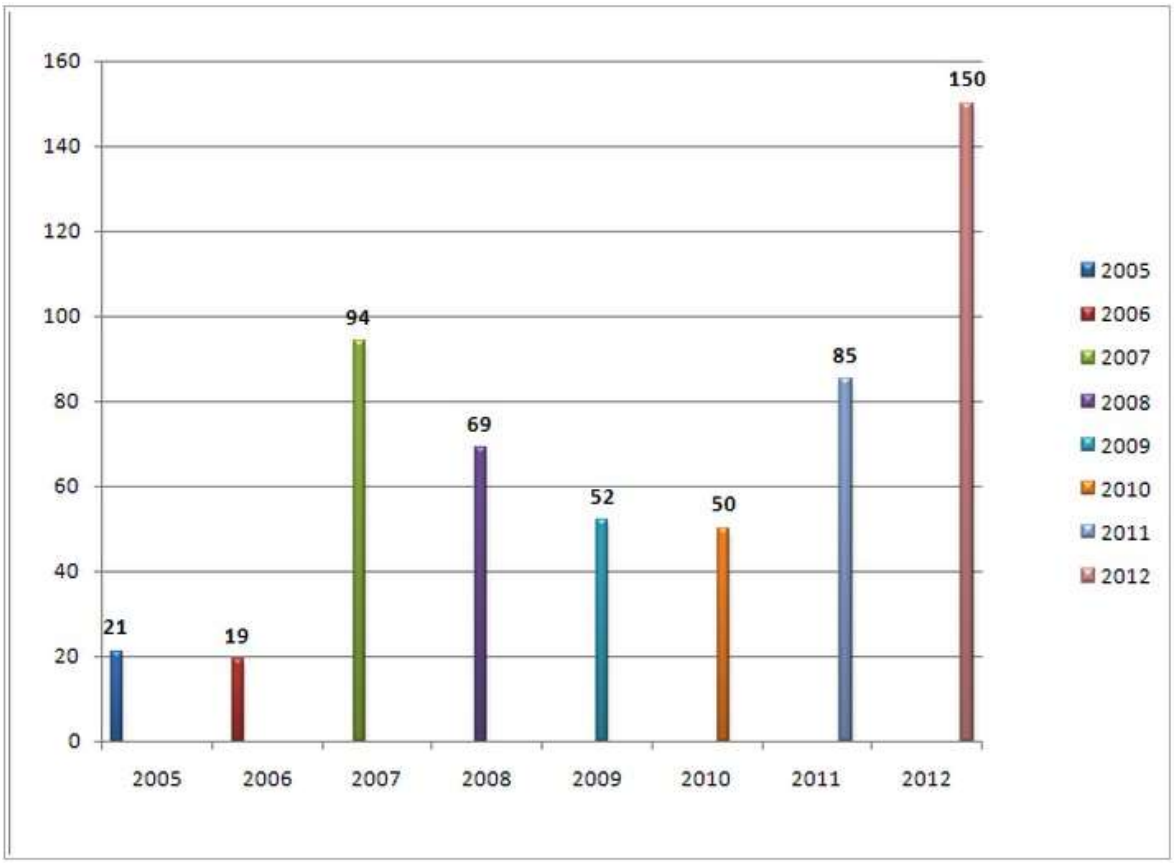
vydání a datum platnosti, název úřadu, který doklad vydal, sérii a číslo průkazu, fotografii a podpis oprávněného držitele průkazu. [11]

4.4 Platební karty

Plastová karta s magnetickým proužkem na rubní straně je dosud používána jako bankovní platební karta (debetní, kreditní). Rozměr karty je stanoven mezinárodní normou41. Magnetický proužek slouží jako médium pro záznam identifikačních údajů potřebných pro provedení platební transakce elektronickým způsobem. Zápis údajů je prováděn na základě magnetického principu, což neposkytuje dostatečné záruky pro bezpečnost jejich používání. Postupně jsou tyto karty nahrazovány kartami čipovými. Plastová karta s magnetickým proužkem na rubní straně je dosud používána jako bankovní platební karta (debetní, kreditní). Rozměr karty je stanoven mezinárodní normou. Magnetický proužek slouží jako médium pro záznam identifikačních údajů potřebných pro provedení platební transakce elektronickým způsobem. Zápis údajů je prováděn na základě magnetického principu, což neposkytuje dostatečné záruky pro bezpečnost jejich používání. Postupně jsou tyto karty nahrazovány kartami čipovými.

Z hlediska zneužití platebních karet patří dle policejních statistik mezi nejčastější metody zneužití z řad rodinných příslušníků, známých a kolegů. Dalším způsobem získání finančních prostředků je skimming. Název je odvozen z angl. data skimming sbírání dat. V roce 2012 došlo k nárůstu počtu případů, kdy bylo zjištěno nasazení skimmovacího zařízení - napadení bankomatů v České republice, oproti předchozímu období. [13]

Graf 3 Případy skimmingu v ČR [13]



4.4.1 Karta s magnetickým páskem

Plastová karta s magnetickým proužkem na rubní straně je dosud používána jako bankovní platební karta (debetní, kreditní). Rozměr karty je stanoven mezinárodní normou41. Magnetický proužek slouží jako médium pro záznam identifikačních údajů potřebných pro provedení platební transakce elektronickým způsobem. Zápis údajů je prováděn na základě magnetického principu, což neposkytuje dostatečné záruky pro bezpečnost jejich používání. Postupně jsou tyto karty nahrazovány kartami čipovými.

4.4.1.1 Magnetický proužek

Je umístěn na zadní straně karty. Jsou na něm uloženy údaje o kartě a jejím držiteli, které jsou nutné pro provedení dané platby či výběru z bankomatu. Magnetický proužek neumožňuje tak vysoké zabezpečení uložených dat jako čip, proto na něm není uložen PIN. Magnetický proužek má tři záznamové stopy, které mají specifický účel.

Obrázek 7 Karta s magnetickým pruhem [14]

Stopa 1 - má 79 znaků, které obsahují číslo karty (až 18 číslic) a jméno klienta (až 26 alfanumerických znaků).

Stopa 2 - obsahuje 40 numerických znaků včetně čísla karty (až 19 číslic) a v bankovnictví se používá nejvíce.

Stopa 3 - na rozdíl od 1. a 2. stopy, které jsou určeny pouze pro čtení, může být záznam na 3. stopě přepisován. Třetí stopa se používala u on - line bankomatů. Finanční limit klienta se snižoval o vybírané částky a po uplynutí stanoveného času se opět navyšoval na původní úroveň. Na této stopě byl zaznamenán parametr, podle kterého bylo možné ověřit správnost kódu PIN. K záznamu potřebných informací sloužilo až 107 numerických znaků (PIN, kód země, měnová jednotka, finanční limit a další). [14,15]

Příklad záznamu:

1. stopa:

%B4406160384321844^NOVOTNY/ZDENEK.MR^02125211652600000000001910000000?;

2. stopa:

4406160384321844=02125211652619120?+

3. stopa:

014406160384321844=20300002000000003050120057131002000021 22=20316216181471803==1=70000000000000000000?

4.4.2 Čipová karta

Plastová karta s magnetickým proužkem na rubní straně je dosud používána jako bankovní platební karta (debetní, kreditní). Rozměr karty je stanoven mezinárodní normou. Magnetický proužek slouží jako médium pro záznam identifikačních údajů potřebných pro provedení platební transakce elektronickým způsobem. Zápis údajů je prováděn na základě magnetického principu, což neposkytuje dostatečné záruky pro bezpečnost jejich používání. Postupně jsou tyto karty nahrazovány kartami čipovými. [15]

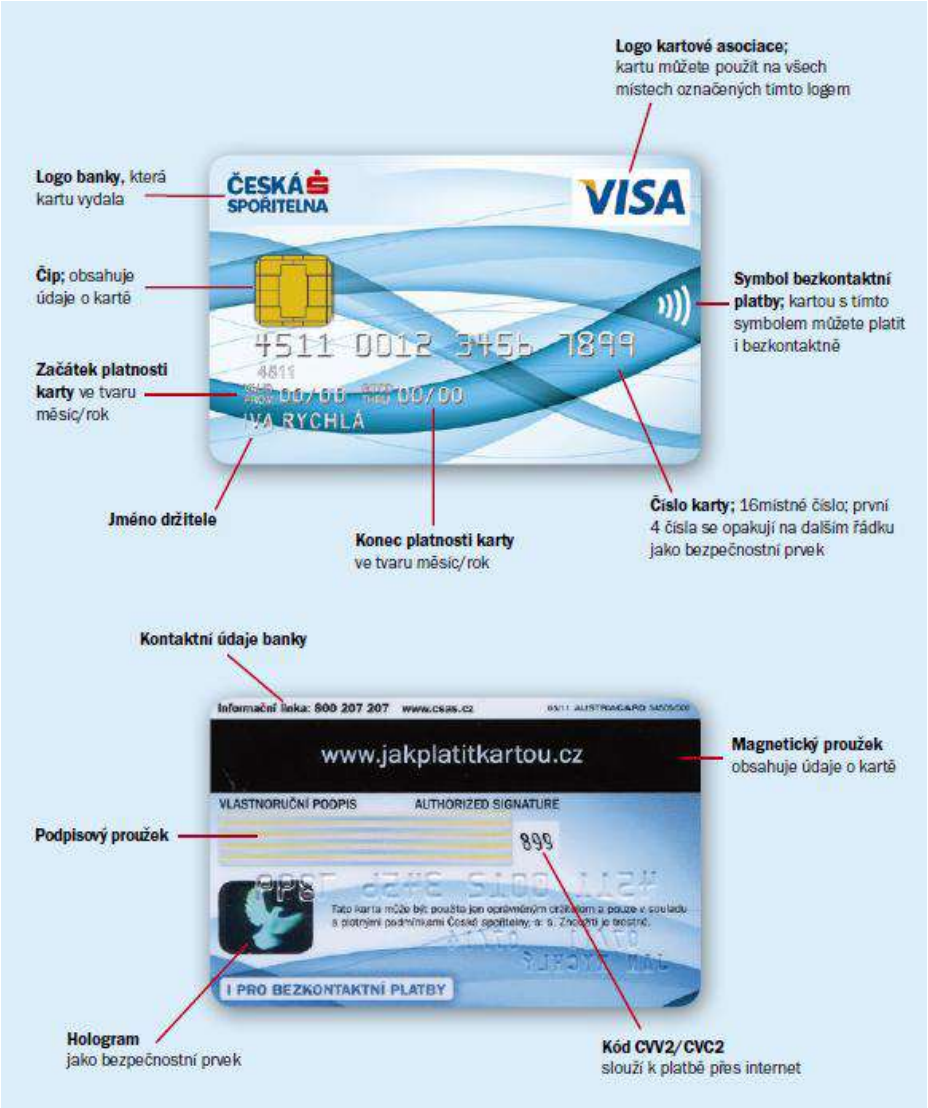
4.4.3 NFC

Jedná se o tzv. NFC (Near Field Communication) bezdrátovou komunikaci, která je založena technologii RFID (Radio Frequency Identification). Ta slouží k přenosu a ukládání dat pomocí elektromagnetických vln. Systémy RFID dokáží zaznamenávat, uchovávat a poskytovat věcné informace v reálném čase. Tento systém je možný aplikovat do různých odvětví a oblastí, kde se klade důraz, na co nejrychlejší a přesné zpracování informací a okamžitý přenos zobrazených dat. Jde o formu bezkontaktní komunikace mezi zařízeními, sloužící pro bezkontaktní platby a jako jsou chytré telefony a tablety. Tato komunikace probíhá na poměrně krátkou vzdálenost od 4 do 20 cm, eventuálně dotykem obou přístrojů. [15]

Obrázek 8 *Bezkontaktní platby [21]*

4.4.4 Hybridní karty

Obsahují jak magnetický proužek, tak i čip. Dnes již všechny banky vydávají pouze tento typ platebních karet, který odpovídá standardu EMV (vychází z normy ISO 7816). Tato zkratka je složena z počátečních názvů asociací Europay, MasterCard a Visa, které stály u zrodu myšlenky čipové platební karty a definovaly standardy toho, jak má taková platební karta fungovat. [15]



Obrázek 9 Technická ochrana platební karty [15]

4.5 Identifikační karty

Identifikační karty slouží pro označení příslušnosti jedinců ke společnosti, ke státu, ke klubu či k nějaké komunitě, či k zájmové skupině osob. Obsah, účel a funkčnost identifikačních karet je velmi různorodá. V řadě států světa je vydávána identifikační karta jako všeobecně povinný doklad občana, jinde jsou vydávány karty označující příslušnost občana na systému pojištění (karta zdravotního nebo sociálního pojištění). V podstatě má však identifikační karta jeden zásadní účel – přiřadit jedinci jednoznačný identifikátor (většinou číselný) pro použití při administrativních úkonech ve styku instituce s jednotlivcem. V ČR se s identifikačními kartami setkáváme především identifikaci studentů či zaměstnanců v návaznosti na další služby systému, jako je např.

- systém kontroly vstupů
- docházkový systém
- stravování
- knihovna

4.6 Zbrojní průkaz

Zbrojní průkaz je doklad, který opravňuje fyzické osoby k nabývání vlastnictví a držení zbraně, případně takovou osobu opravňuje k nošení takové zbraně. K jeho získání je podobně jako u řidičského oprávnění třeba splnit určité zákonem stanovené podmínky. Zbrojní průkaz lze v určitých situacích použít k prokázání totožnosti držitele, neboť je vedle uvedení jména, příjmení, data narození a místa trvalého pobytu rovněž vybaven podobiznou oprávněného držitele. [14]

4.7 Služební průkaz

Služební průkazy deklarují příslušnost jejich držitele k určité organizaci či úřadu. Jsou-li takové doklady opatřeny fotografií jejich držitele, mohou být spolu s dalšími údaji uvedenými v průkazu použity jako doklady k prokázání totožnosti. Služebním průkazem zpravidla prokazuje zaměstnanec či příslušník existenci pracovního nebo služebního poměru vůči zaměstnavateli či úřadu a někdy i z těchto důvodů vyplývající oprávnění provádět určité činnosti a úkony. [15]

4.8 Údaje k identifikaci osob

Za identifikační údaj můžeme považovat každou informaci, která vede k určení totožnosti konkrétní fyzické osoby. Jednou ze základních skupin takových informací jsou údaje o jménu a příjmení, tedy údaje přidělené osobě volním aktem. Dalším druhem informací jsou základní údaje, které jsou evidovány jako jednou zjištěné, vyplývající z určité existující skutečnosti. Těmi jsou například číselné hodnoty a zeměpisné údaje. Takové informace jsou úředně přidělovány a předepsaným způsobem zaznamenávány patřičnými evidenčními orgány a jsou tedy spravovány státem. Třetí skupinu identifikačních údajů fyzických osob tvoří arbitrárně a náhodně přidělované údaje. [32]

4.8.1 Jméno a příjmení

Podstata, struktura a původ lidmi používaných jmen úzce souvisí s kulturním, náboženským, regionálním a legislativním prostředím. Jméno a příjmení můžeme jednoznačně označit jako základní identifikační údaj. Právo na ochranu těchto základních identifikačních údajů, tedy jména a příjmení, máme všude tam, kde jsou tyto údaje uváděny spolu s dalšími osobními údaji, se zákonem stanovenými výjimkami. [32]

4.8.2 Datum a místo narození

Datum a místo narození fyzické osoby jsou informace, které jsou zcela jednoznačné a přesně určitelné. Jinými slovy, vždy se dá určit, kdy a kde se fyzická osoba narodila a z logiky věci je jasné, že takové údaje jsou nezaměnitelné a jedinečné, tedy osoba se vždy narodila v jeden konkrétní den a na jednom konkrétním místě. Proto jsou tyto informace ideální pro používání jako identifikačních údajů fyzické osoby. Datum a místo narození osoby jsou identifikační údaje, které jsou každému subjektu přiděleny jako údaje vyplývající z nějaké určité existující skutečnosti a jsou tedy prakticky neměnné. [32]

4.8.3 Rodné číslo

Rodné číslo bylo zavedeno pro statistické a evidenční účely a je definováno jako identifikační charakteristika obyvatele. Určuje ho zásadně okresní oddělení Českého statistického úřadu (ČSÚ). Pro zabezpečení určitých činností je zákonem stanoveno, ve kterých případech se rodné číslo musí oznamovat. Používání rodného čísla jako jednoznačného identifikátoru v jiných případech se vžilo, avšak často je v rozporu se zákonem. Rodné číslo (u občanů narozených do 31. 12. 1953 devítimístné, u občanů narozených od 1. 1. 1954 desetimístné) tedy slouží ke zjednodušení identifikace občanů České republiky. Rodná čísla osobám narozeným do 31. 12. 1968 vydává MPSV – Česká správa sociálního zabezpečení, rodná čísla osobám narozeným od 1. 1. 1969 vydává Český statistický úřad, od 1. 1. 2003 přiděluje RČ ministerstvo vnitra11. RČ je tvořeno z data narození ve tvaru RRMMDD u ženského pohlaví se k hodnotě MM přičítá 50. Závěrečné trojčíslí má povahu sekvenčního čísla a posledním místem je kontrolní znak. Z uvedené

struktury vyplývá, že RČ má poměrně značnou vypovídací schopnost:

- den, měsíc a rok narození (poslední dvě číslice roku narození)
- identifikace pohlaví (rozlišuje měsíc narození – u žen plus 50)
- číslice za lomítkem je pořadové číslo přidělené na každý den k místu narození

Při zavedení rodného čísla nebylo jeho používání nijak legislativně upraveno. Toto číslo začalo být postupně používáno ve všech situacích, kdy bylo potřeba jednotlivce jakkoliv identifikovat. A to i v situacích docela banálních, kdy identifikace nebyla ani nutná či potřebná. Navíc se toto číslo, pro svou technickou strukturu, začalo všeobecně používat jako třídící klíč ve většině databází týkajících se jednotlivců. Vznikla tak možnost tyto databáze provázat a sdílet právě prostřednictvím rodného čísla. Nekontrolované propojování databází přineslo zásadní problémy z pohledu ochrany soukromí jednotlivců. Náprava tohoto stavu bude velmi dlouhá a obtížná. Při přechodu na jiný identifikátor je třeba vzít v úvahu i jiné systémy než jsou systémy státní správy, které využívají RČ jako jednoznačný (i když nikoliv jediný) identifikátor (např. bankovní systémy, účetní systémy, evidenční systémy, atd.). Zde všude by se musela provést pravděpodobně úprava, která by si vyžádala ve svém důsledku značné náklady. Rodné číslo se hojně využívá jako defaultní heslo k přihlášení informačním systémům, jako příklad lze uvést portál (portal.utb.cz), což je webová aplikace, která integruje různé informační systémy (je napojena na datové zdroje) a umožňuje uživateli přístup k různým údajům centralizovaně na jednom místě a pod jednou identitou - tedy pod jediným přihlášením. [17,18]

Obrázek 10 Vytvoření rodného čísla [32]

4.8.4 Identifikátor sociálního zabezpečení

V České republice je Ministerstvem práce a sociálních věcí (MPSV) používán tzv. Identifikátor klienta MPSV (IK) a to k identifikaci osob, které jsou zapsány v Informačním systému státní sociální podpory MPSV (klienti SSP) a v Informačním systému služeb zaměstnanosti MPSV (klienti Úřadů práce). Toto číslo je desetimístné, nikdy nezačíná nulou, a na rozdíl od rodného čísla neobsahuje žádnou vnitřní informaci. Z důvodu nezaměnitelnosti s rodným číslem se pro Identifikátor klienta MPSV nevyužívají hodnoty, které by se jako RČ mohly interpretovat. Identifikátor klienta MPSV se osobě přiděluje prostřednictvím kontaktního místa SSP (Státní sociální podpora) nebo Úřadu práce. Toto číslo používá MPSV také při vydávání certifikátů pro zaručený elektronický podpis. [12]

4.8.5 Identifikátor zdravotního pojištěnce

Nositeli čísla zdravotního pojištěnce jsou všichni účastníci pojištění na všeobecném zdravotním pojištění v České republice. Tento identifikátor je shodný s rodným číslem občana. Odlišnosti mohou vzniknout u osob se stejným rodným číslem nebo u osob, kterým nebylo rodné číslo přiděleno. V těchto případech přiděluje číslo zdravotního pojištěnce Všeobecná zdravotní pojišťovna ČR (VZP ČR).

Problematikou elektronického identifikátoru zdravotního pojištěnce jako nástroje pro přesnou evidenci pojištěnců, pro bezpečnou komunikaci s pojištěncem a zvýšení informovanosti pacienta, pro vytvoření možnosti sdílení technické a datové infrastruktury mezi zdravotními pojišťovnami a souvisejícími agendami v rámci veřejné správy, zejména pak v oblasti státní sociální podpory, zaměstnanosti a sociálního zabezpečení, se VZP ČR zabývá již dlouhou dobu. Od roku 2004 VZP ČR začala vydávat svým pojištěncům nové identifikační průkazy podle jednotného grafického a obsahového vzoru EU – Evropského průkazu zdravotního pojištění (EHIC – European Health Insurance Card), který nahrazuje formulář zdravotního pojištění. Od 1. 1. 2006 jsou tímto průkazem pojištěnce vybaveni všichni pojištěnci v ČR, bez rozdílu příslušnosti ke zdravotní pojišťovně. Na rozdíl od předchozího papírového průkazu pojištěnce VZP, obsahuje nový průkaz pojištěnce také identifikační číslo průkazu, podle něhož lze zjistit, kterému pojištěnci byla konkrétní karta vydána. Číslo průkazu vydaného pojištěnci je evidováno v identifikační databázi pojištěnců. [12]

Obrázek 11 Evropský průkaz zdravotního pojištění [19]

4.8.6 Identifikační čísla osob

Identifikace pomocí čísel, vyjadřujících určitý kód, směřuje ke zpřesnění zjištění a určení totožnosti subjektu. V České republice se jako identifikační číslo fyzické osoby používá tzv. rodné číslo. Vedle rodných čísel se k identifikaci fyzické osoby rovněž užívá daňová identifikační čísla, čísla účtů u finančních institucí, evidenční čísla průkazů sloužících jako veřejné listiny, atd. Smyslem číslování pomocí přidělovaných identifikačních čísel a kódů jako jedinečných znaků je zajištění vysoké přesnosti, efektivity a jednoznačnosti při následné či opakované identifikaci. Díky těmto kódům není dále nutné používat rozsáhlé popisné texty a doplňující charakteristiky. Je zcela zřejmé, že na efektivitu využívání číselných identifikačních údajů má klíčový vliv ucelený a fungující systém jejich přidělování, stejně tak kvalitní a spolehlivý způsob vedení jejich evidence.

5 VIRTUÁLNÍ IDENTITA

S pojmem virtuální identita se setkáváme ve vazbě s informačními systémy a lze jej definovat jako trvalý a jednoznačný datový profil, který je používán konsistentně a je tudíž pro ostatní osoby identifikovatelný bez toho, aby bylo možné poznat původní fyzickou osobu.

Z právního hlediska není identita přesně definována, nicméně pojem identity používá. Např. Zákon o ochraně osobních údajů operuje s pojmem "určenost" či "určitelnost" atributů, které nelze zaměnit s jiným subjektem.

Virtuální identitu bychom však měli chápat i v širším kontextu. Není to jen identifikace reálné osoby v kyberprostoru, ale bývá to prezentace osoby ve virtuálním životě. Stejně jako v realitě, i v kyberprostoru je identita tvořena mnoha faktory (názory, vystupování), které ji specifikují.
Naše virtuální identita je charakterizována především identifikačními prvky: [18]

- přihlašovací jméno/heslo u webové aplikace
- e-mailová adresa (neanonymní)
- telefonní číslo
- osobní číslo v zaměstnání
- doménové jména
- hesla

V elektronickém světě se krádeží identity rozumí zejména neoprávněné užívaní nekalým způsobem získaných hesel, kódů, uživatelských jmen, případně i bezpečnostních předmětů včetně platebních karet a elektronických průkazů. Smyslem je provedení transakce – elektronické komunikace jménem jiné osoby, zpravidla za účelem obohacení (převod finančních prostředků, získání chráněných informací), ale i například za účelem poškození dobrého jména (použití firemního e-mailu).

Nejcitlivěji je tato problematika vnímána ve finančním sektoru, kde terčem zájmu útočníka jsou přihlašovací a ověřovací údaje s cílem neoprávněně manipulovat s finančními prostředky oběti. To ovšem neznamená, že by se jiných oblastí problém netýkal. Stejně tak se může jednat o možné zneužití přístupu k uživatelským účtům poskytovatelů

telekomunikačních služeb, utilit, ale i databázových celků veřejné správy (katastry, evidence) s dálkovou formou přístupu. Samostatnou kapitolou by bylo zneužití elektronického podpisu při podání (daňového přiznání, správní řízení), podvržení právních úkonů činěných elektronicky, uzavírání spotřebitelských smluv a specificky smluv o finančních službách prostředky elektronické komunikace na dálku. Jedná se o vážná rizika v oblasti bezpečí klientských dat či finančních prostředků, která ovlivňují i důvěryhodnost elektronické komunikace.

V dnešní době sféra hackingu dospěla do dalšího stupně: hackeři mohou hledat důvěrné informace ve veřejně přístupných online profilech uživatelů. Lidé tráví stále více času v blozích, online komunitách a na stránkách společenských sítí, jako jsou MySpace, Facebook, Twiter, nebo Tagged. Uživatelé si zde tvoří vlastní profily a často v nich prezentují své koníčky, domácí mazlíčky, oblíbené celebrity nebo týmy – a příslušná slova se běžně používají také jako hesla. Uživatelé sociálních sítí jsou zvyklí na neformální komunikaci a nedovedou posoudit legitimnost komunikující strany nebo např. hypertextových odkazů a ve své důvěřivosti se mohou stát obětí podvodu.

Podobně tomu může být při účasti v online diskusních skupinách, blozích nebo při komunikaci přes instant messengery, jako je ICQ, GoogleTalk, Viber či Jabber. Tato prostředí přinášejí pocit nezávazné konverzace, a mohou tak být zdrojem citlivých informací. Někdy i zdánlivě základní informace mohou hackerům stačit ke krádeži citlivých osobních údajů. Tak jako v reálném světě záleží na nás, komu otevřeme dveře, s kým se bavíme a komu důvěřujeme, záleží i v online světě na nás, s kým chceme komunikovat a jaké informace mu poskytneme. Online svět je svět tak trochu pro sebe a citlivé osobní údaje do něj nepatří. [19]

Obrázek 12 Schéma virtuální identity [vlastní]

6 VIKTIMOLOGICKÉ ASPEKTY, PROFIL PACHATELE A LEGISLATIVA

6.1 Viktimologie

Oběti trestné činnosti spočívající v nelegálním získání a následném zneužití identifikačních osobních údajů se obvykle dostávají do velmi složité situace. To je dáno zejména tím, že krádež jejích identity je mnohdy provedena velmi sofistikovaným způsobem (pokud nejde o prosté odcizení osobních dokladů, platebních karet, listinných dokumentů apod.) při využití počítačových dat a systémů a celý průběh viktimizace se odehrává ve virtuální oblasti. Oběť mnohdy pozná, že došlo ke zneužití její identity, až se značným časovým odstupem. Škody, které oběti vzniknou, někdy nelze zpočátku rozpoznat jako důsledek trestné činnosti, ale mohou být považovány za důsledek administrativního omylu, nedostatků v evidenčních systémech, za selhání byrokratického aparátu apod. Důkazní břemeno tak spočívá na oběti, která se sama musí domáhat nápravy stavu umožňující trestnou činnost, kterou byla poškozena. Z hlediska viktimologie, můžeme důsledky způsobené krádeží identity třídit na:

- přímé finanční škody - včetně ztráty úspor; náklady na zjištění a předcházení finančních škod; náklady na obnovení důvěry
- nepřímé finanční škody - včetně snížení ratingu peněžních ústavů; poškození obchodní a profesní pověsti; zápis do policejních evidencí
- psychologické důsledky – ty značně závisí na tom, jak byly identifikační údaje zneužity; může jít i o existenční důsledky pro celou rodinu, jejíž člen se stal obětí zneužití identity
- závažné důsledky jde tehdy, když zneužití identity vede k další trestné činnosti, jako je například terorismus, obchodování s lidmi, drogová kriminalita.

V moderní společnosti, kdy každý jedinec i instituce vstupují do složitého přediva vztahů, povinností a oprávnění, se stává ochrana a zachování vlastní identity naléhavou nezbytností. Viktimnost, tedy riziko, že se staneme obětí trestné činnosti ohrožující a zneužívající naše identifikační data, je vysoká.

Lze říci, že v České republice byly vytvořeny dostatečné zákonné podmínky pro náležitý trestní postih kriminality spojené s odcizením a zneužitím identifikačních dat. [1]

Z pohledu práva je krádež identity považována za dvoustupňový trestný čin.

1. Pachatel musí nejprve získat cizí počítačovou identitu. Děje se tak nejčastěji odcizením elektronických dat (hesla, přístupové údaje atd.), a to zpravidla neoprávněným kopírováním dat (skimming), lstivým vylákáním údajů (phishing) či nedovoleným vniknutím do cizího počítače (hacking). Jedná se o tzv. identity theft.
2. V druhé fázi pachatel zneužije neoprávněně nabytou identitu. Cílem bývá vesměs majetkový prospěch, tzv. identity fraud. Z právního hlediska se jedná o klasický podvod a judikatura v tomto směru přizpůsobuje výklad novým informačním technologiím. V řídkých případech může být cílem pouhé poškození oběti, např. tím, že bude pod jeho jménem vystupovat v sociálních sítích typu Facebook, a může se dopustit např. trestného činu poškozování cizích práv. [20]

6.2 Profil pachatelů

Kapesní zloději – v souvislosti s krádeží identity se jedná o problematiku spadající do kategorie sociální identity, tedy krádeže fyzických dokladů. Zpravidla se jedná o organizované skupiny, pocházející ze zemí východního bloku. Pachatelé se snaží na sebe neupozorňovat, pohybují se v prostorách s větším výskytem osob (prostředky veřejné dopravy, zastávky, koncerty), kde mají ideální podmínky k páchání trestné činnosti.

Úvěrové podvody – v tomto případě se opět může jednat jak o jednotlivce, tak o organizované skupiny. Využívají technik sociálního inženýrství. Typickým příkladem můžou být nabídky ¨výhodnějších¨ úvěrů, telefonních služeb, či nabídky z oblasti energetiky. Zpravidla se jedná se o komunikativní osoby ve věku 25 – 35 let.

Hacker – talentovaný, inteligentní (zpravidla vysokoškolsky vzdělaný) programátor, který by mohl vyřešit téměř jakýkoliv problém v oblasti informatiky. Mají malou schopnost citových vazeb s jinými lidmi. Typickými znaky může být sebestřednot, intelektuální arogance a netrpělivost. Hackeři, které neřadíme do kategorie organizovaného zločinu, berou tvorbu škodlivých softwarů spíše jako výzvu, kterou upřednostňují před finančními zisky. [22]

6.3 Legislativa

Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod

Listina se skládá ze 44 článků členěných do šesti hlav. Nacházíme v ní základní lidská práva a svobody, politická práva, dále hospodářská, sociální a kulturní práva, práva národnostních a etnických menšin a práva na soudní a jinou právní ochranu.

Zákon č. 121/2000 Sb., autorský zákon

Autorský zákon upravuje tzv. autorská práva. To jsou práva autorů k jejich dílům. Dílo je zákonem definováno jako literární a jiné dílo umělecké a dílo vědecké, které současně je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě. Dílem je např. dílo slovesné (např. román), grafické (např. kresba), hudební (např. znělka), choreografické (např. baletní choreografie), fotografické, audiovizuální (např. film), architektonické (stavba) nebo počítačový program. Autorským dílem není pouhý nápad nebo myšlenka, dílo musí být vyjádřeno tak, aby jej někdo jiný mohl vnímat. Od tohoto okamžiku je dílo chráněno autorským právem, není tedy nutná žádná registrace, jako např. u patentů. [23]

Zákon č. 227/2000 Sb., o elektronickém podpisu

Tento zákon upravuje v souladu s právem Evropských společenství[1)] používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem. [23]

Zákon č. 101/2000 Sb., o ochraně osobních údajů

Kde se za osobní údaj považuje jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu. [23]

Zákon č. č. 328/1999 Sb., o občanských průkazech

Zákon upravuje vydávání občanských průkazů státním občanům České republiky způsob prokazování totožnosti a vedení agendového informačního systému, práva a povinnosti držitelů a evidenci občanských průkazů. [23]

Zákon č. č. 329/1999 Sb., o cestovních dokladech

Zákon upravuje vydávání cestovních dokladů státním občanům České republiky, jejich používání občany a vedení agendového informačního systému evidence cestovních dokladů, práva a povinnosti držitelů a agendového informačního systému evidence diplomatických a služebních pasů. [23]

Zákon č. 361/2000 Sb., o provozu na pozemních komunikacích

Pro naše potřeby zákon upravuje vydávání, práva a povinnosti držitelů řidičského oprávnění. Definuje o oprávnění k řízení motorových vozidel zařazených do příslušné listiny nebo podskupiny řidičského oprávnění a kterou držitel prokazuje své jméno, příjmení, rodné číslo a podobu, jakož i další údaje v ní zapsané. [23]

Právní ochranu můžeme hledat najít v trestním zákoníku, kde v souvislosti s danou problematikou můžeme definovat tyto trestné činy:

- **Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 TZ)**

  Jedná se o nový trestný čin, který spočívá v neoprávněném získání přístupu k cizímu počítači, a to tím, že pachatel překoná bezpečnostní opatření. Může se jednat o jakékoli bezpečnostní opatření, tzn. postačí i prolomení jednoduchého hesla. Výhodu lze spatřovat ve skutečnosti, že nemusí dojít k vlastní krádeži dat, ale stačí pouhé zajištění si přístupu k cizímu počítači. [23]

- **Porušení tajemství dopravovaných zpráv (§ 182 TZ)**

  Již Listina základních práv a svobod zajišťuje každému listovní tajemství. Trestní zákoník konkretizuje tento rozsah a zakazuje komukoli porušit tajemství zpráv určených konkrétní osobě, které jsou posílány prostřednictvím sítě elektronických komunikací (v zásadě telefoničtí operátoři). Nikdo rovněž nesmí porušit tajemství neveřejného přenosu počítačových dat po počítačovém systému. V každém případě je třeba prokázat úmysl pachatele. [23]

- **Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 TZ)**

  Zde se jedná o jakékoli nakládání se zařízením, softwarem, databází hesel apod., které umožňují spáchat jeden z výše uvedených trestných činů, nebo o jejich výrobu. Je ovšem třeba prokázat úmysl pachatele. Smyslem je zamezit jakékoli podpoře této trestné činnosti a rozšířit okruh odpovědných osob - trestný čin zahrnuje i pouhé přechovávání či zprostředkování takovýchto zařízení. [23]

- **Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 TZ)**

  Tento trestný čin volá po odpovědnosti konkrétních osob, které nakládají s důležitými údaji a způsobí ztrátu nebo změnu počítačových dat. Ke spáchání tohoto trestného činu postačí hrubá nedbalost vyplývající ze zaměstnání či funkce. Je však nutné, aby vznikla minimálně značná škoda, tj. škoda v minimální výši 500 tisíc Kč. [23]

II. PRAKTICKÁ ČÁST

7 PODVODNÉ PRAKTIKY – SOCIÁLNÍ IDENTITA

Jedná se o podvodná jednání, kterých se pachatel dopouští na základě předložení falešných či pozměněných dokladů např. potvrzení o příjmu, výpis z běžného účtu nebo odcizených či padělaných dokladů totožnosti při sjednávání smlouvy. Do žádosti jsou uvedeny nepravdivé informace nebo hrubě zkreslené informace. Údaje v žádosti se vztahují zejména k jeho zaměstnavateli, výši příjmu, zda je klient ve zkušební výpovědní lhůtě, či výši jeho závazků.

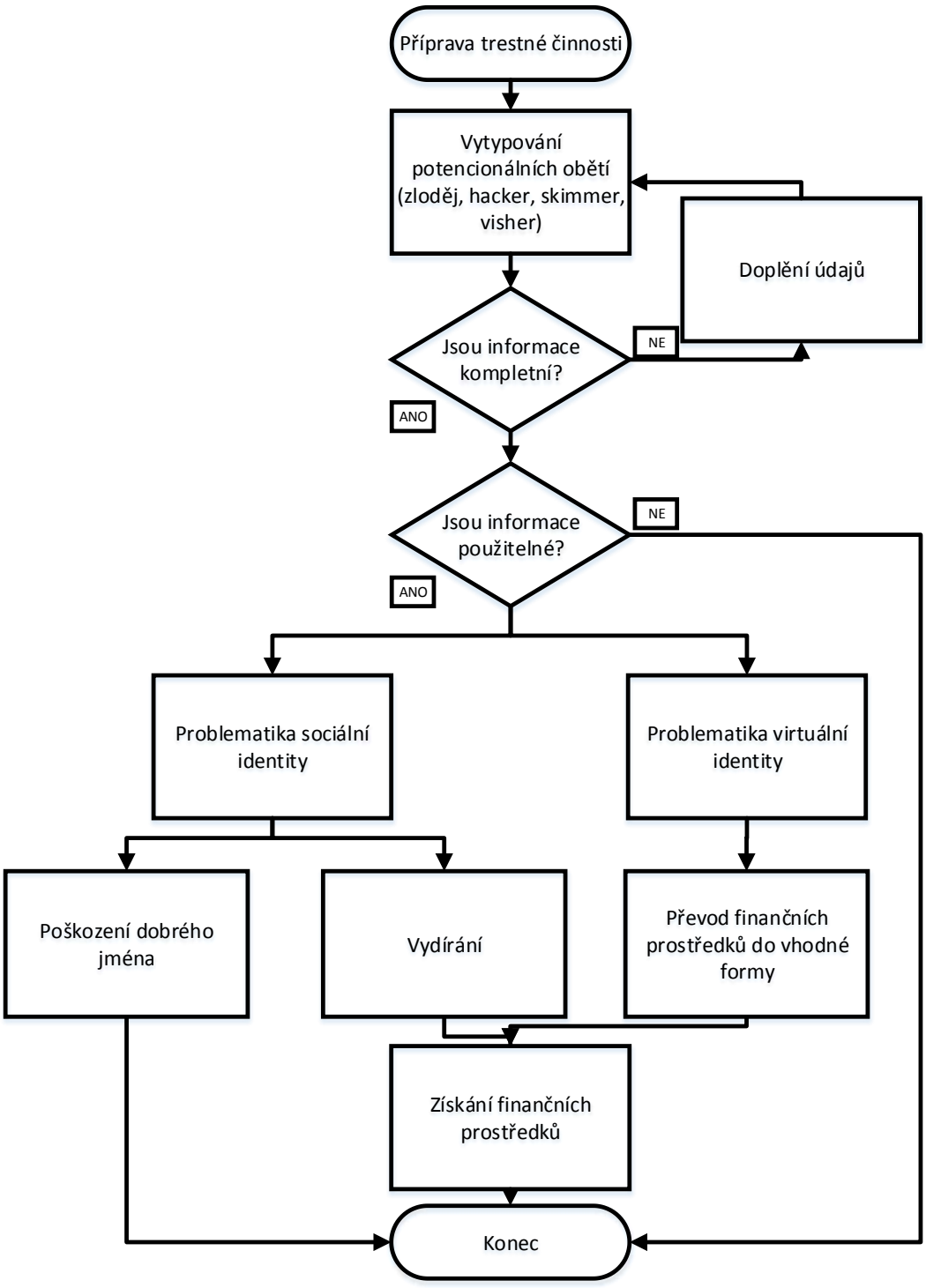
Smlouva je uzavřená bez vědomí (přítomnosti) klienta na padělané, pozměněné, odcizené nebo ztracené doklady (občanský průkaz, řidičský průkaz, cestovní pas). Padělanými doklady se rozumí nepravé doklady, které byly plně vyhotoveny pachatelem a mají vyvolat dojem, že byly vydány příslušným orgánem a předepsaným způsobem. Pozměněnými doklady se rozumí pravé doklady, na něž byla učiněna změna údajů o skutečnostech, který pravý doklad osvědčuje (přepsání údajů, výměna fotografie).

Prostředky, jimiž si pachatel opatřuje osobní údaje, se liší ve smyslu jejich technické náročnosti. Některé z těchto aktivit jsou trestnými činy téměř ve všech zemích (např. krádež), některé nikoliv. Mezi nejobvyklejší způsoby získávání osobních údajů k pozdějšímu použití k trestné činnosti patří: [24]

Typickými příklady zneužitá osobních dokladů jsou:

- Nákup na půjčky bez ručitele.
- Výběr cizího bankovního konta.
- Půjčení auta.
- Nákup zbraní.
- Rezervace hotelových pokojů.
- Zavírání smluv s mobilními operátory.
- Vstup do prostor organizace.

Průběh krádeže identity jak fyzickou tak virtuální cestou znázorňuje vývojový diagram:



Obrázek 13 Průběh krádeže identity [vlastní]

7.1 Příklad průběhu krádeže identity

1. Pachatel získal osobní údaje tak, že na internetu inzeroval nabídku poskytnutí nebankovní půjčky a od zájemce vylákal fotokopie občanského a řidičského průkazu a výpisu z účtu (vedeného u jiné banky na zájemcovo jméno).

2. Takto získané kopie dokumentů pak pachatel zaslal bance, u níž si chtěl na cizí jméno založit účet. Banka pachateli spolu s číslem jeho nově založeného účtu sdělila, že účet aktivuje až poté, co na něj pachatel zašle alespoň jednu korunu z jeho již existujícího účtu. Tím bance podle zákonem stanovených pravidel potvrdí shodu identifikačních údajů s údaji na zaslaných kopiích.
3. Ke splnění této podmínky pachatel vyzval zájemce o nebankovní půjčku, aby ze svého účtu převedl na konkrétní účet (který pachateli nově založila banka) alespoň jednu korunu. Po připsání platby banka zasláním klíče a hesla k internetovému bankovnictví pachateli umožnila ovládání účtu, aniž by původní zájemce o nebankovní půjčku o existenci účtu založeného na jeho identitu vůbec věděl.
4. V konečné fázi podvodu pak pachatel již jen sdělil žadateli, že mu půjčka nebyla poskytnuta, a další komunikaci s ním přerušil. [25]

7.2 Doporučená protiopatření

Důležitá je stejně, jako i v ostatních případech prevence. Je třeba si uvědomit, že organizované skupiny i jednotlivý pachatelé, mají tento druh trestné činnosti předem velmi dobře připravený a tak je nezbytné, minimalizovat riziko potenciální ztráty.

- Okamžité nahlášení ztráty osobních dokladů. Je třeba si uvědomit, že přestože je osobní doklad veden v databázi ministerstva vnitra jako odcizená, je možné s ní podvodně manipulovat. Pokud je už ovšem zablokovaný, uživatel se tím zříká odpovědnosti za případné škody.

Tabulka 1 Kam nahlásit ztrátu/odcizení dokladů [vlastní]

	Ztráta	Odcizení
Občanský průkaz	Úřad s rozšířenou působností	Policie ČR
Řidičský průkaz	Úřad s rozšířenou působností	Policie ČR
Cestovní pas	Úřad s rozšířenou působností	Policie ČR
Platební karta	v bance, která kartu vydala	Policie ČR
Zbrojní průkaz	Policie ČR	Policie ČR
Služební průkaz	u organizace, která průkaz vydala	Policie ČR (vyžadováno v některých případech)
Identifikační karty	u organizace, která kartu vydala	Policie ČR (vyžadováno v některých případech)

- Dohled nad osobními věcmi
- Opatrné nakládání s rodným číslem – které slouží jako identifikátor v řadě institucí, např. v nemocnici, na finančním úřadu nebo ve třeba ve zdravotní pojišťovně. Přes

jedno číslo je tak o možné získat spoustu dalších údajů o majetku, zdraví nebo financích.

- Nosit peněženku, doklady a kartami zvlášť
- Nedávat osobní doklady a platební karty z ruky
- Nepořizovat kopie nebo skeny osobních dokladů
- PIN platební karty nemít uložený v mobilním telefonu či napsaný v blízkosti karty
- Vytvořit seznam kontaktů pro informování či blokování při ztrátách

7.3 Zneužití platební karty - skimming

Označení pro podvodné jednání, při kterém pachatelé (padělatelé platebních karet) zkopírují údaje z magnetického proužku platební karty bez vědomí jejího právoplatného držitele. Tyto údaje pachatelé zneužijí tím, že je následně nahrají na předem připravený nosič dat – padělek platební karty.

Ke zkopírování informací z platebních karet nejčastěji dochází:

- u bankomatů, kde podvodníci prostřednictvím speciálního kopírovacího zařízení zkopírují všechna data z magnetického proužku platební karty a použijí je rovněž k výrobě padělku (tento způsob skimmingu je nejrozšířenější);
- u obchodníků, kde nepoctivý pracovník obchodní společnosti zkopíruje údaje z magnetického proužku platební karty před vrácením zákazníkovi a takto získané údaje použije nebo dále předá k výrobě padělku platební karty (k uvedenému podvodnému jednání dochází nejčastěji v barech, restauracích, někdy na čerpacích stanicích nebo v hotelech). [26]

Skimmovací zařízení je technické zařízení umožňující zkopírování elektronických údajů z platební karty. Taková zařízení bývají nejčastěji nainstalována pachateli na bankomaty v místech pro vkládání karty. Skládají se z části, která načítá data z platební karty vložené do bankomatu a části, která umožňuje získat číselný PIN kód. Pouze získání obou těchto údajů umožní osobám, které nelegálně kopírují údaje z platební karty, následnou výrobu padělků karet a nelegální výběry z finančních účtů v ČR i v zahraničí.

Obrázek 14 Bankomat se skimmovacím zařízením a falešnou klávesnicí [26]

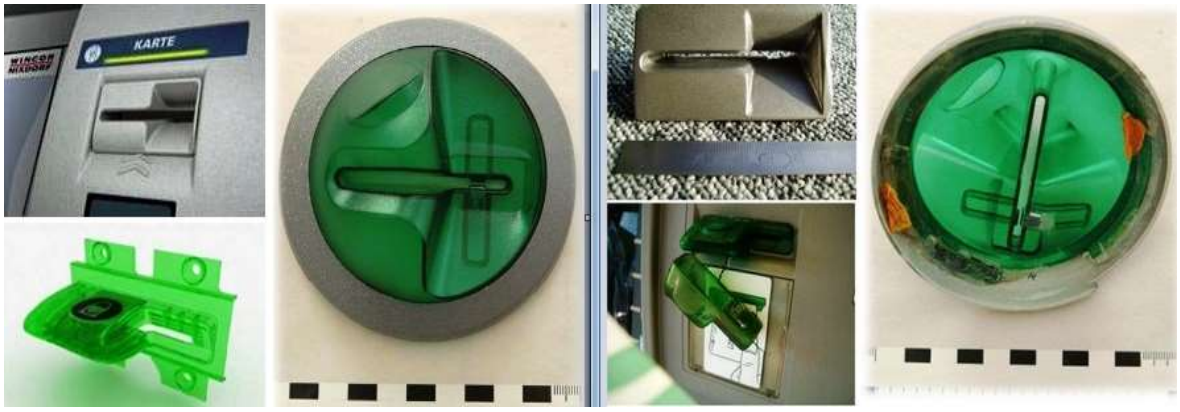
7.3.1 Provedení skimmovacího zařízení

Skimovací zařízení je v podstatě čtečka dat, uložených na magnetickém proužku platební karty, která je schopna záznamu do vlastní paměti. Lépe vybavená zařízení jsou schopna posílat bezdrátově přečtená data. Je možné zařízení naprogramovat na různé funkce. K odesílání dat okamžitě po jejich přečtení, odeslání dat až po zaplnění paměti apod. Zařízení je složeno z několika částí, které jsou v plastovém krytu. K řízení slouží mikroprocesor, k ukládání dat flash paměť. Čtení dat probíhá pomocí čtecí hlavy (se třemi pruhy). Toto základní vybavení v lepších modelech doplňuje modul pro bezdrátovou komunikaci.

Kopírovací zařízení nainstalována přímo na štěrbinu pro vkládání karty formou různých nástavců napodobujících originál nebo formou panelu, který bývá montován na originální součást bankomatu. Pachatelé využívají horní panel bankomatu pro umístění minikamery (velikost řádově v mm) k odpozorování PIN kódu nebo bývá používána falešná klávesnice, která je samostatně nebo formou celého panelu montována na originální klávesnici či panel bankomatu. [26]

Kopírovací zařízení a krycí lišty kopírovacích prostředků na bankomatech jsou vesměs provedeny v barvě a kovu velmi podobných materiálů, ze kterých je bankomat vyroben. Při zběžném pohledu jsou tato zařízení od originálu téměř nerozpoznatelná, Detekovat v místě zneužitého bankomatu je můžeme podle viditelný známek neodborné montáže

(obrázek 11), způsobené nedostatkem časových možností, které pachatel při instalaci skimmovacího zařízení má.



Obrázek 15 Antiskimmingový nádstavec a neodborná montáž [26]

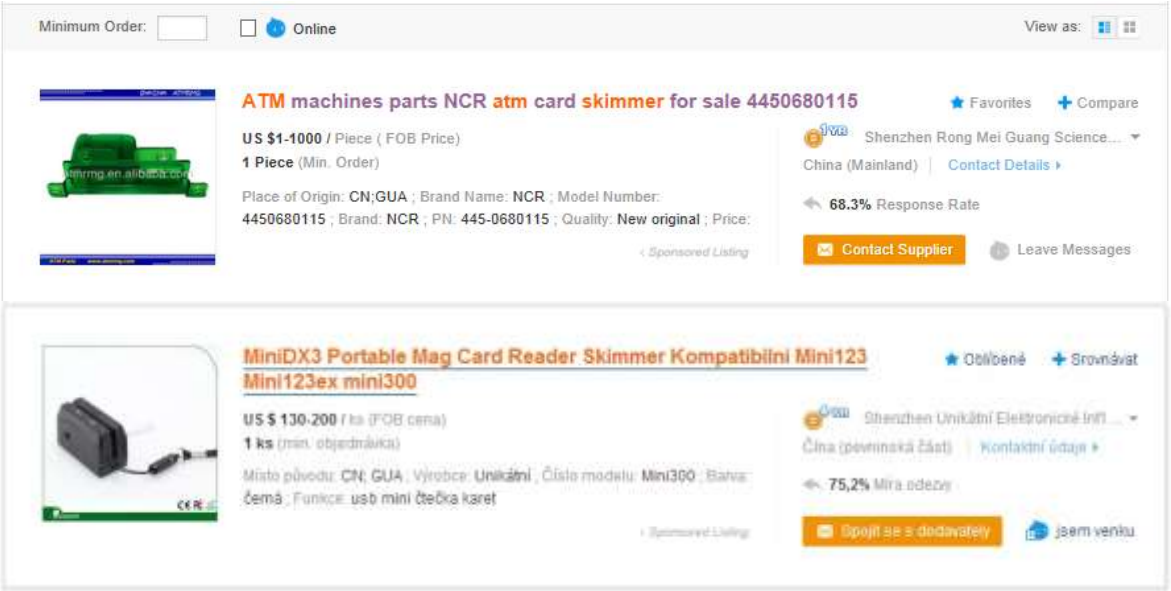
7.3.2 Způsoby podvodného získání PIN kódu

Vedle údajů z magnetického proužku je dalším důležitým údajem pro pachatele skimmingu PIN kód. K jeho zjištění (odpozorování) využívají pachatelé v případě bankomatů kamery, mobilní telefony nebo speciální klávesnici, která může být umístěna na klávesnici nebo místo klávesnice původní. [27]

Obrázek 16 Falešná klávesnice + kamera [26]

7.3.3 Dostupnost skimmovacích zařízení

Zařízení se nachází v několika verzích. Využívá se vždy zařízení s totožnou primární funkcí jen s různým technickým vybavením. Většina těchto zařízení je možné koupit prostřednictvím internetu z nejrůznějších míst světa. Jako příklad uvádím nabídku skimmovacích zařízení internetového obchodu z Číny (www.alibaba.com). Uvedené zařízení obsahuje 2MB paměť a slouží k uložení až 3000 záznamů a přenos dat pomocí portu USB.



Obrázek 17 Dostupnost skimmovacích zařízení [27]

7.3.4 Bezpečnost platebních karet a ochrana před skimmingem

Bankovní společnosti uplatňují řadu preventivních opatření před kopírováním karet, jakými jsou např. instalace zařízení proti kopírování a softwarů v bankomatech, preventivní blokování karet v případě podezření na skimming, spolupráce s policií a monitoring bankomatů. Přesto ke skimmingu dochází, a proto by se měl každý z nás chovat při nakládání s platební kartou obezřetně. [27]

- Uchování PIN kódu v naprosté tajnosti (nesdělovat jiné osobě, nezaznamenávat v mobilním telefonu, na kartě, v dokladech, nebo dokonce v blízkosti karty apod.).
- Při výběru z bankomatu dbát zvýšené pozornosti místu, kde výběr se provádí (zaměřit se na nejbližší okolí a pohybující se osoby, důkladně si bankomat prohlédnout, zda na něm nejsou provedeny konstrukční změny a úpravy).
- Pro výběr finančních prostředků z bankomatu volit raději frekventované a dostatečně osvětlené místo.
- Při zadávání číselné kombinace PIN kódu na klávesnici zakrýt část základní desky s čísly druhou rukou (tímto způsobem se zabrání možnému odpozorování číselné kombinace).
- Při transakci neztratit kontrolu nad kartou a nenechat se nikým a ničím ovlivnit.

- Transakci neuskutečnit při podezření, že něco není v pořádku.
- Kontrola výpisů transakcí proti prodejním a výplatním dokladům (sledování možného výskytu neoprávněných transakcí).
- Při podezření, že je na bankomatu umístěno skimmovací zařízení, neprodleně informujete Policii ČR prostřednictvím linky 158, popřípadě bankovní společnost (kontaktní infolinka bývá na bankomatech umístěna).
- Při platbě kartou v restauraci či prodejně dbát, aby platební transakce proběhla pod dohledem osoby, která kartu vlastní (personál by neměl kartu nikam odnášet).

7.4 Ztráta, krádež a útoky na mobilní zařízení

Současná mobilní zařízení již nepředstavují jen pouhé jednoúčelové přístroje, nýbrž díky vysokému výpočetnímu výkonu, operačnímu systému a nejrůznějším typům implementovaných komunikačních technologií se stávají součástí každodenního života mnoha lidí. To však sebou přináší i rizika, úzce související s danou problematikou. Je třeba si uvědomit, že data, která se v mobilním zařízení nachází, jsou srovnatelná s těmi, která se nachází v počítači a notebooku, přičemž krádež mobilního telefonu či tabletu je pro pachatele běžnou rutinou. Mezi informace, které se v telefonu nebo na paměťové kartě nachází, patří například:

- Telefonní kontaky
- Soukromá komunikace SMS
- Emailová komunikace
- Fotky, videa
- Přístup ke sdíleným složkám (Dropbox)
- Uložená hesla
- Přístup na sociální sítě

Skutečnost, že současná mobilní zařízení jsou vybavena operačními systémy, dala příležitost vzniku novým druhům útoků. Jedná se o útoky prostřednictvím tzv. škodlivého software neboli (malware), v podstatě jisté obdoby těch, známým ze světa osobních počítačů.

7.4.1 Prevence mobilních útoků

Uživatelé ve většině případů pro zabezpečení informací v mobilních telefonech nedělají obvykle mnoho nebo prakticky nic což je způsobeno úzkou vazbou mezi samotným hardwarem a na něm běžícím softwarem) na druhé straně se ale možnou ztrátou zařízení a zneužití svých dat obávají.

V rámci každého mobilního operačního systému lze identifikovat určitá potenciální slabá místa a z toho plynoucí rizika. I v tomto případě, stejně jako jindy platí, že základní prevencí napadení zařízení je právě dostatečná informovanost uživatele o potenciálních hrozbách souvisejících s používáním konkrétního mobilního zařízení a možnostech jak jim předejít. V tomto kontextu se jedná především o udržování operačního systému ve stále aktuální podobě, disciplinovanost a zodpovědnost při práci s webovým prohlížečem, uvážené stahování aplikací, a též výběr vhodného antivirového programu. [31]

7.5 Obnovení vyhozených dokumentů - trashing

Jde o cílený útok na osobu či organizaci. Představuje další metodu způsobu podvodů, která se opět snaží získat citlivé údaje. Název pochází z anglického výrazu trash (koš), protože zdrojem dat jsou obvykle vyhozené dokumenty ať už v podobě fyzické či elektronické. Tato praktika spočívá ve shromažďování neskartovaných informaci, které obsahují osobní údaje týkající se oběti, např. číslo kreditní karty, bankovního účtu či cestu k adresáři, získání, podpisového vzoru. [34]

7.5.1 Ochrana před trashingem

Ochrana je v tomto případě zřejmá. Je nutné dbát pozornost na řádnou skartaci dokumentů a zabezpečení jejich odvozu či případné skladování, a to jak ve fyzické tak v elektronické podobě. Při volbě podpisového vzoru je mnohem bezpečnější takový, který je odlišný od běžně používaného podpisu klienta, nebo který je doplněný o zvláštní markant, který klient běžně nepoužívá.

8 PODVODNÉ PRAKTIKY – VIRTUÁLNÍ IDENTITA

Jde o útoky, které využívají neznalosti, chyb a sociálního cítění uživatelů. Snaží se pod záminkou vystupování pod smyšlenou institucí nebo osobou vylákat z uživatelů citlivé informace vedoucí k přístupu do prostředí internetového bankovnictví zneužité osoby.

8.1 Viry a škodlivý software

Počítačový virus je malý softwarový program, který se šíří z jednoho počítače do druhého a překáží provozu počítače. Počítačový virus může poškodit nebo odstranit data v počítači, pomocí e-mailového programu se rozšířit do dalších počítačů, nebo dokonce odstranit celý obsah pevného disku.

Počítačové viry se často šíří prostřednictvím rychlých zpráv nebo příloh e-mailových zpráv. Proto se nedoporučuje otvírat přílohu e-mailu, pokud se neví, kdo zprávu odeslal. Viry mohou být maskovány jako přílohy obsahující vtipné obrázky, pohlednice nebo zvukové soubory či soubory videa. Počítačové viry se také šíří při stahování z Internetu. Počítačové viry se mohou skrývat v nelegálním softwaru či v jiných souborech nebo programech, které stáhnete.

Malware - z angl 'malicius software', česky škodlivé programy. Sem zahrnujeme spyware, adware, rootkity, trojské koně, viry a červy. Adware a malware jsou podle projevů škodlivého kódu, zatímco trojské koně wormy a viry jsou kategoriemi dle způsobů šíření

Spyware - z angl 'spy' - špion, zvěd. Jeho úkolem je z počítače zaznamenávat stisky kláves, vyhledávat čísla kreditních karet, hesla, dělat screenshoty a získávat další informace z napadeného počítače.

Adware - z angl. 'advertisement' - reklama. Velmi oblíbená aktivita obzvláště červů a trojských koní. Zobrazování nevyžádané reklamy v oknech prohlížeče, přesměřování domácí stránky, nebo dokonce nahrazuje reklamní bannery vlastními. Toto dělá např. trojský kůň, který nahrazuje informace v reklamě vlastními.

Rootkit - rootkitem rozumíme takový program, který mění chování operačního systému za účelem skrytí určitých dat - souborů, obsah paměti, příp. registru. Účelem je zakrýt jiný program tak, aby bylo ztíženo ostatním programům jej najít a příp. odstranit. Nejčastějšími skrývanými objekty jsou trojské koně, ovšem rootkity použila i firma Sony jako součást hudební ochrany.

Trojský kůň - program, který se snaží předstírat, že je užitečný, ale hlavním účelem je nainstalovat nějaký škodlivý kód. Od virů se liší tím, že svůj škodlivý kód neumí zkopírovat do jiného souboru. Mohou být typu spyware i adware.

Červ - angl 'worm' - aktivní škodlivý kód, který využívá chyb zabezpečení, a umí se šířit bez pomoci uživatelů skrz počítačové sítě. Prvním známým červem byl tzv. Morrisův červ. Červ se může chovat sám jako spyware, nebo může provést zavedení trojského koně.

Virus - škodlivý kód, který se vyskytuje uvnitř souborů. Umí vložit do spustitelného souboru, po jehož spuštění se snaží modifikovat kopií svého kódu další souboru. Dále existují i tzv. bootviry, což jsou viry, u nichž se škodlivý kód ukládá do boot sektoru na disku. Představují největší riziko poškození dat, pokud se antivirovému programu nepodaří škodlivý kód odstranit.

Exploity - zneužívá nově zjištěných či jinak nezabezpečených slabých míst software. Obvykle využívá operačního systému, webového prohlížeče nebo programu, který se rutinně aktivuje prostřednictvím webového prohlížeče. [40]

8.2 Antiviry

Proti těmto škodlivým kódům se možné zamezit pomocí antivirů, které sleduje všechny nejpodstatnější vstupní/výstupní místa, kterými by viry mohly do počítačového systému proniknout. Lze je rozdělit na:

On-demand skenery - spouštějí se přes rozhraní OS DOS a jsou určeny pro případ, že systém není z důvodu poškození schopen nastartovat běžným způsobem.

Jednoúčelové antiviry - jde o antivirové programy, které jsou zaměřeny na detekci, popřípadě i odstranění jednoho konkrétního viru, popřípadě menší skupiny virů. Tyto antiviry vznikají většinou k likvidaci rozšířeného viru v dané době.

Antivirové systémy - jde o komplexní antivirové řešení, které má za úkol ochránit počítač před červy šířící se poštou, škodlivými skripty případně zabránit stažení infikovaných souborů. Komplexní nástroj může mít ve výbavě firewall a další specializované nástroje. [40]

8.3 Firewall

Česky něco jako „bezpečnostní brána“, je zjednodušeně řečeno zařízení či software oddělující provoz mezi dvěma sítěmi (naší domácí a internetem), přičemž propouští jedním nebo druhým směrem data podle určitých předem definovaných pravidel. Brání tak zejména před neoprávněnými průniky do sítě a odesílání dat ze sítě bez vědomí a souhlasu uživatele. V prostředí domácností a malých firem je instalace brány firewall nejefektivnějším a nejdůležitějším prvním krokem při ochraně počítače. Je důležité, aby firewall a antivirový software byly zapnuty ještě před připojením k Internetu. Ochrana počítače v místě jejího připojení k internetu, tedy přímo na hranici sítě, pomůže odvrátit většinu hlavních útoků, které přicházejí zvenčí. Ze zkušenosti však víme, že mnohé dnešní velmi promyšlené a výkonné systémy, které používají hackeři a další útočníci, mohou proniknout i přes firewally, a proto je důležitá právě sekundární ochrana jednotlivých počítačů. [40]

8.4 Sociální inženýrství

Pracuje na základě psychologického podtextu pro získání důvěrných informací, které mohou být dále zneužity počítačovým pirátům pro spáchání trestného činu. Sociální inženýrství se zaměřuje na nejslabší článek informační bezpečnosti, kterou představuje samotný člověk. Útočník zneužívá lidskou neopatrnost, nevědomost, lehkovážnost při používání Internetu, aby se dostal k uživatelovým údajům, které by mohl zneužít ve svůj prospěch. Základním prvkem sociálního inženýrství je manipulace. Útočník se vydává za instituce, společnosti nebo osoby, které opravdu existují.

8.5 Phishing

Jde o šíření falšovaného e-mailu příjemci, který klamavým způsobem napodobuje legální instituci (banku či organizaci) ve snaze vyzvědět od příjemce důvěrné informace jako číslo platební karty, PIN, CVV kód nebo číslo bankovního účtu. Takový e-mail navádí uživatele, aby navštívil webové stránky či odpověděl na příchozí zprávu a předal tak nevědomky důvěrné informace, které pak pachatel využije pro svůj prospěch. V České republice jde nejčastěji o útoky na klienty České spořitelny, v celosvětovém měřítku se pak hackeři zaměřují především na společnosti jako PayPal, eBay, Barclays Bank. [37]

Tabulka 2 Útoky na společnosti [38]

Pořadí	Značka
1.	PayPal
2.	eBay
3.	Barclays Bank
4.	Bank of America
5.	Fifth Third Bank
6.	JPMorgan Chase
7.	Wells Fargo
8.	Volksbanken Raiffeisenbanken
9.	Branch Banking and Trust
10.	Regions Bank

Nemusí jít jen o bankovní účty, ale také účty ostatních organizací, kde dochází k manipulaci s penězi nebo je možné jakýmkoliv způsobem zneužít jejich služeb.

Pavel Hubáček

Od: Bonny Henri <debt@multlock.cz>
Odesláno: 13. května 2014 14:30
Komu: webmaster@fame.utb.cz
Předmět: Výše pohledávky na vašem účtu #4545530312288092
Přílohy: smlouva_30573B3393A122373.zip

Vážený zákazníku,

Jsme velmi rádi, že jste využívali produktu z naší banky.
Dovolujeme si Vás upozornit na dlužnou částku ve výši 8257.10 Kč,ke dni 13.04.2014 na osobním účtě #4545530312288092 . Nabízíme Vám uhradit pohledávku v plné výši do 20.05.2014.

Dobrovolné uhrazení pohledávky a dodržení smlouvy #30573B3393A122373 umožňujeme Vám:
1) Dodržet pozitivní úvěrovou historii
2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.

V případě prodlení úhrady pohledávky 8257.10 Kč v souladu s platnými právními předpisy, jsme oprávněni zahájit právní sankci na základě pohledávky.

Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor "smlouva_30573B3393A122373.zip"

S pozdravem,
Vedoucí odboru vymáhání pohledávek
Bonny Henri
+420 606 113 609

Obrázek 18 Phishingový email [vlastní]

Typickými znaky phishingového e-mailu:

- snaží se vyvolat dojem, že byl odeslán organizací, z jejíchž klientů se snaží vylákat důvěrné informace. Tohoto se snaží docílit grafickou podobou e-mailu a zfalšováním adresy odesílatele
- text může vypadat jako informace o neprovedení platby, výzva k aktualizaci bezpečnostních údajů, oznámení o dočasném zablokování účtu či platební karty, výzkum klientské spokojenosti nebo jako elektronický bulletin pro klienty
- v textu zprávy je link, který na první pohled většinou vypadá, že směřuje na stránky banky. Ve skutečnosti ale odkazuje na jiné místo, kde jsou umístěny podvodné stránky
- jestliže klient klikne na odkaz v e-mailu, dostane se na falešné stránky podvodníků, které jsou vytvořeny ve stejném stylu, jako originální stránky banky. Na podvodných stranách je připraven formulář, kde jsou požadovány důvěrné informace – čísla účtu, kódy k internetovému bankovnictví, PIN k platební kartě, přihlašovací údaje ke službám apod. [41]

8.5.1 Hlavička e – mailu

Hlavička poskytuje informace, od koho email přišel, komu byl určen, jaký je předmět zprávy a kdy byla zpráva odeslána. Jde o důležitou součást emailu, neboť podle jejích údajů se řídí servery, přes které zpráva prochází.

```
Received: from sun.utb.cz (195.178.88.66) by EXCHANGE1.fame.utb.cz
 (195.178.93.110) with Microsoft SMTP Server id 14.1.438.0; Tue, 13 May 2014
 14:30:32 +0200
Received: from sun.utb.cz (localhost [127.0.0.1])       by nod32.utb.cz (Postfix)
 with ESMTP id 37B23340939D7;    Tue, 13 May 2014 14:30:39 +0200 (CEST)
X-Virus-Scanner: This message was checked by ESET Mail Security
        for Linux/BSD. For more information on ESET Mail Security,
        please, visit our website: http://www.eset.com/.
Received: by sun.utb.cz (Postfix, from userid 1000)     id 33972340939E2; Tue, 13
 May 2014 14:30:39 +0200 (CEST)
X-Spam-Checker-Version: SpamAssassin 3.2.3 (2007-08-08) on sun.utb.cz
X-Spam-Level:
X-Spam-Status: No, score=0.0 required=5.0 tests=none autolearn=ham
        version=3.2.3
Received: from rs.cesnet.cz (rs.cesnet.cz [195.113.144.199])    by sun.utb.cz
 (Postfix) with ESMTP id 86D7F340939D7  for <webmaster@fame.utb.cz>; Tue, 13
 May 2014 14:30:22 +0200 (CEST)
Received: by rs.cesnet.cz (Postfix, from userid 1001)   id 7B0BE1A40237; Tue, 13
 May 2014 14:30:22 +0200 (CEST)
X-Greylist: delayed 00:15:57 by SQLgrey-1.8.0-rc2
Received: from keosciji.keretom.ru (ppp37-190-56-4.pppoe.spdop.ru
 [37.190.56.4]) by rs.cesnet.cz (Postfix) with SMTP id C1AAE1A4022C     for
 <webmaster@fame.utb.cz>; Tue, 13 May 2014 14:30:14 +0200 (CEST)
Message-ID: <2087888830@skol.cz>
Date: Tue, 13 May 2014 16:30:12 +0400
From: Bonny Henri <debt@multlock.cz>
X-Mailer: Petrolic v7.4
MIME-Version: 1.0
To: <webmaster@fame.utb.cz>
Subject: =?utf-8?b?VsO9xaFlIHBvaGxlZMOhdmt5IG5hIHZhxaFlbSDDusSNdHUgIzQ1NDU1MzAzMTIyODgwOTI=?=
Content-Type: multipart/mixed; boundary="----------B563FD681A4209BC"
Return-Path: debt@multlock.cz
X-MS-Exchange-Organization-AuthSource: EXCHANGE1.fame.utb.cz
X-MS-Exchange-Organization-AuthAs: Anonymous
```

Obrázek 19 Hlavička emailu [vlastní]

8.5.2 Ochrana proti phishingu

Pokud uživatel bude opatrný (dávat si pozor kam klikám) a používá aktualizovaný antivirový program a firewall, nehrozí mu prakticky žádné nebezpečí. Důležité je neuveřejňovat své osobní údaje na internetu- ať už v diskusních fórech, na svých osobních stránkách, nebo v nezabezpečené komunikaci. Google umí většinu z těchto údajů vyhledat a útočník je neváhá použít. Mezi základní opatření, která platí před zneužití citlivých dat phishingem patří:

- Neklikat na odkazy v e-mailu, které přesměrují uživatele na podvodné stránky, které se ho mohou snažit oklamat a pokusit se vylákat důvěryhodné informace, ale také mohou obsahovat škodlivé kódy, které se pokusí instalovat do počítače
- Používání aktualizovaného operačního systému. V aktualizacích bývají opravené objevené bezpečnostní chyby, které jinak mohou být zneužity. Většina systémů umí, při správném nastavení, kontrolovat aktualizace sama.
- Použití antivirového programu a jeho pravidelné aktualizace. Existují kvalitní antivirové programy, které jsou pro domácí použití zdarma, případně je možné zakoupit i komerční produkty. Pokud je počítač připojený k Internetu, dokáže si

antivirový program (při správném nastavení) stáhnout aktualizaci sám. Neaktualizovaný antivir nemusí včas odhalit nové viry.

- Použití antispywarových programů a firewall. Antispywarové programy dokáží odhalit další druhy škodlivého software. O jejich aktualizaci platí totéž, co v předchozích případech. Firewall chrání před nežádoucím přístupem zvenčí nebo může zabránit odchozímu spojení pochybných programů do Internetu.
- Nespouštějte neznámé programy a přílohy, které přijdou e-mailem, ani na které e-mail odkazuje! Je třeba dodržovat nejvyšší opatrnost, přestože zpráva může vypadat, že je od vašich nejbližších přátel. Typickým příkladem jsou různé podvržené odkazy na elektronické pohlednice. Ve skutečnosti se nekalé živly snaží z odkazované stránky nainstalovat do počítače škodlivý program. Například kromě popisované funkčnosti mohou obsahovat i trojské koně, které pracují ve prospěch svých tvůrců.
- K elektronickému bankovnictví nebo k účtům (nejen bankovním) se nepřihlašovat z veřejně přístupných nebo nedůvěryhodných počítačů. Mohou být na nich nainstalovány různé programy pro monitorování činnosti a vaše důvěrné informace nebo přístupové kódy se mohou dostat k neoprávněným osobám. Toto se týká nejen počítačů v internetových kavárnách, ale také třeba i u známých, kde jsou instalovány programy z různých zdrojů a nemáte jistotu jejich zabezpečení.
- Jestliže není možné, mít svůj osobní počítač, který nesdílíte s ostatními členy rodiny, je vhodné vytvořit účty pro každé uživatele (pokud možno, ne s právy administrátora). Získáte tím částečnou ochranu před nežádoucími úpravami systému.
- Použití zdravého rozumu a úsudku. I přes veškeré technologické zabezpečení se může objevit jednoduchý trik, kterým se může nechat uživatel snadno obelstít. Jestliže nebude dodržovat základní bezpečnostní pravidla a nepřemýšlet nad svojí činností, můžete se stát další obětí.
- V případě, že se jedná o útoky na emailové schránky v podnikové síti, je vhodné, aby administrátor informoval zaměstnance o hrozícím nebezpečí

8.5.2.1 Vishing

Je další metodou phishingu, ale s rozdílem, že místo zaslání emailu jsou uskutečňovány telefonní hovory, které žádají čísla kreditních karet, PIN kódů apod. Zločinec konfiguruje „válečné vytáčení“ (vytáčení série telefonních čísel). Útočník tedy ve většině případů vystupuje jako zaměstnanec banky. Pokud útočník úspěšně získal přihlašovací údaje klienta do internetového bankovnictví, poslední překážkou k převedení peněz zůstává autorizační kód. Útočník může telefonicky

kontaktovat klienta a představit se jako zaměstnanec jeho banky. Oznámí mu, že na jeho účtu jsou prováděny podezřelé finanční transakce. Aby si zajistil důvěru, uvede klientovo přihlašovací jméno i heslo. Poté mu oznámí, že na jeho telefon bude zaslána autorizační SMSs kódem, který musí klient zadat nebo zaslat na telefonní číslo, které mu útočník nadiktuje. Oklamaný klient tak útočníkovi pomůže autorizovat převod vlastních finančních prostředků ze svého účtu.

Tato metoda našla uplatnění především u osob staršího data narození, kterým připadá hlasová komunikace důvěryhodnější než e-mailová zpráva. [42]

8.5.2.2 Smishing

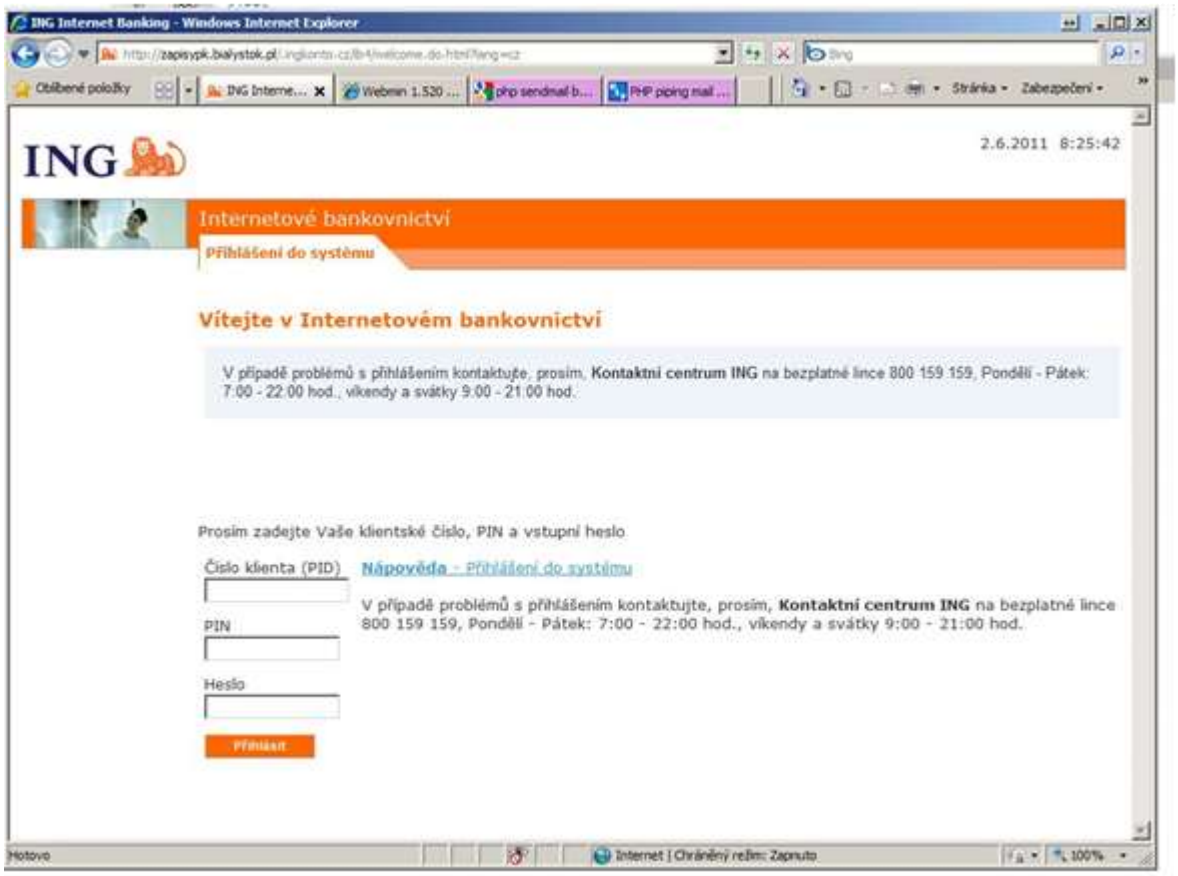
Varianta phisnihgu, ve které jsou k získání informací použity SMS zprávy, a útočník tak zpravidla vystupuje pod hlavičkou banky, pojišťovny, úřadu nebo organizace. Uživatel obdrží SMS zprávu, která ho vláká na telefonní čísla nebo provedení bankovních převodů za různými účely. Odesílatel zprávy je také odesílatel spamů, která se snaží převzít identitu známého, kolegy nebo společnosti ze seznamu kontaktů. Oběť např. obdrží SMS zprávu říkající, že si předplatila on-line datovací službu, nebo jinou službu, a že tato služba bude připsána k účtu za telefon. Zpráva také nabízí spojení k webovým stránkám z telefonu pro přerušení služby. Mnoho lidí provedou propojení, aby odvolali službu. Oběti se poté dostanou tam, kde chce podvodník a může být vystaven nedobrovolnému stahování trojského koně nebo jiného druhu podvodného programu. Jinou metodou je zaslání SMS zprávy, říkající, že banka provedla velkou platbu z účtu oběti, na kterou neexistují dostatečné prostředky. Při zavolání je oběť konfrontována sérii zaznamenaných zpráv, které ji vedou k tomu, aby uvedla podrobnosti bankovního účtu. [42]

8.6 Pharming

Modernější a nebezpečnější technika získávání citlivých informací nese název pharming a je označována za novou generaci phishingu. Stejně jako phishing (se kterým má mnoho společného) a jiné sociotechnicky, slouží k oklamání uživatele. Používá při tom však mnohem sofistikovanější metodu, jak toho dosáhnout.

Princip spočívá v napadení DNS systému. DNS neboli Domain Name System (/Server/Service) je databáze obsahující seznam URL a jim odpovídajících IP adres.

Zajišťuje překlad mezi IP adresou a URL konkrétní webové stránky. Místo těžko zapamatovatelného čtyřčíslí odděleného tečkami, nám dovolí do adresového řádku napsat snáze zapamatovatelný název námi požadovaného serveru. Tedy např. místo 194.50.240.198 – www.csas.cz. [43]



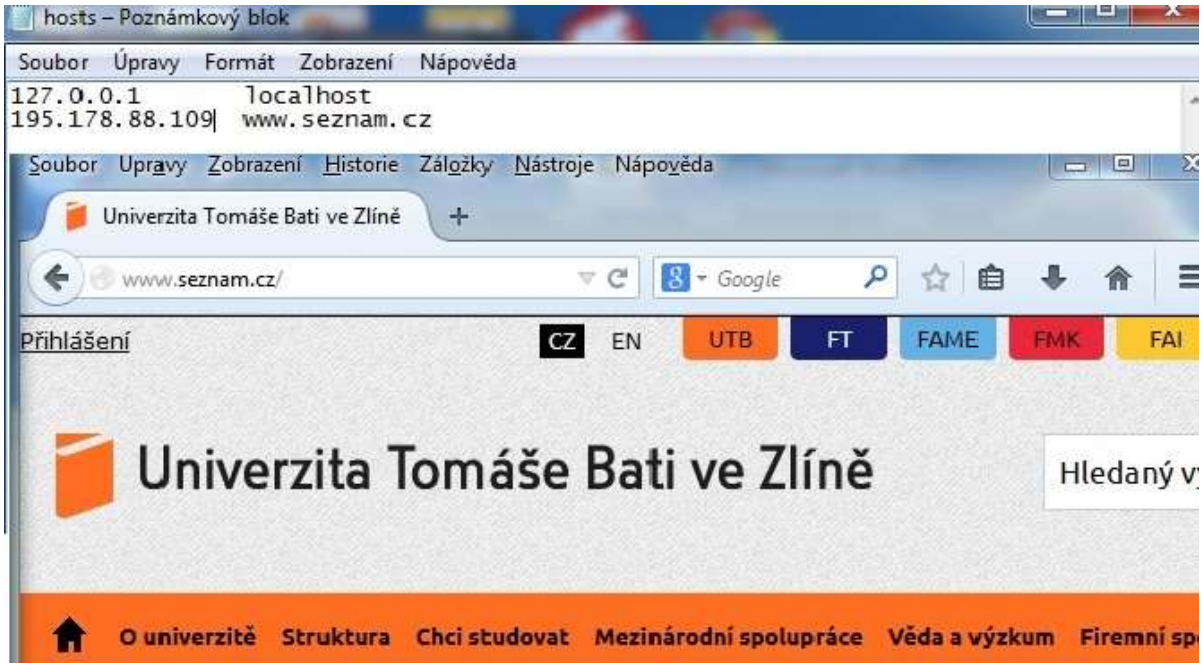
Obrázek 20 Pharming [vlastní]

Pharmingový útok, tak spočívá v přesměrování požadované webové stránky, na stránku falešnou, minimálně se nelišící od originálu. Toho může být docíleno dvěma způsoby. První možností jak toho dosáhnout, je změnou položky v seznamu překladů na nějakém z

DNS serverů, což by vedlo k tomu, že u všech uživatelů, kteří zadají ve svém webovém prohlížeči konkrétní adresu a připojí se na tento DNS server, nedojde k překladu na odpovídající IP adresu, nýbrž na útočníkem podvrženou. Tato metoda není závislá na klientských počítačích, avšak je potřeba zdolat ochranu DNS serveru.

8.6.1 Příklad pharmingu

Jednodušší verze pharmingů lze provést v operačním systému Windows modifikací souboru hosts. Ten se ve většině přídadů nachází v adresáři. C:\WINDOWS\System32\drivers\etc, který je lokální alternativou DNS serverů. V něm se nacházejí IP adresy a jim korespondující URL. Jako ukázku jsem zvolil přesměrování z URL www.seznam.cz na www.utb.cz. Výpis i následná změna jsou znázorněny na obrázku. Stejným způsobem může pachatel provést převedení jakýchkoli adres. Změnu v tomto souboru, může útočník provést skrze druh malwarového programu.



Obrázek 21 Pharming pomocí souboru hosts [vlastní]

8.6.2 Ochrana před pharmingem

Samotné přepsání údajů zajišťují různé počítačové viry, např. trojští koně, kteří se do počítače uživatele dostanou např. v e-mailech nebo v softwaru, který si instaluje, nebo z internetu. Soubor hosts je možné i uzamknout, to ale může způsobovat problémy při běhu některých síťových aplikací. Z toho plyne, že jedinou a nejúčinnější obranou proti tomuto způsobu útoku

je použití kvalitního antivirového systému a jeho pravidelná aktualizace. Cestu k zisku potřebných dat může ztížit správně nakonfigurovaný firewall, nicméně obrana proti pharmingu je v konečném měřítku poměrně složitá.

8.7 Spoofing

Jde o jisté maskování uživatele v síti. Nejčastěji využívanou formou je IP spoofing, který falšuje IP adresu paketů. Pokud je na server odesílán paket s pozměněnou IP adresou odesílatele, nedokáže zachytit odpověď serveru. Proto je možné techniku využívat při jednostranné komunikaci se serverem, nikoli při oboustranné. Spoofing se může využívat i u mobilních telefonů, kde jde o stejné zamaskování autora zpráv. Slovo Spoofing významem vystihuje vtip a jisté napálení cílové osoby. Velice často se spoofing využívá k vedení útoku na nějaký server. Například při útoku DoS (Denial of Service) maskuje spoofing odesílatele paketů, které zahlcují server. Díky němu se může uživatel v síti vydávat za někoho jiného. Není potom těžké zneužít cizí práva. Náchylné jsou potom i služby využívající IP adresu jako ověření uživatele. Spoofing se využívá především při rozesílání reklamních emailů. Zajistí anonymitu odesílatele, která při oslovení většího počtu lidí určitě přijde vhod. Anonymní email je hodně žádaný. Odesílatel ale nesmí zapomínat na jednostrannost spoofingu a počítat se ztrátou zpětné vazby.

8.7.1 Obrana proti spoofingu

Filtrování paketů nám alespoň zajistí částečnou ochranu. Kde ale tohle filtrování paketů probíhá? Bezpečnost našeho počítače je zásluhou firewallu. Jestliže máme ochranný štít zapnutý, firewall obvykle blokuje pakety přicházející z vnějšku, které mají adresu nacházející se ve vnitřní síti.

Firewall by měl také kontrolovat odchozí pakety. U odchozích paketů kontroluje adresu, která by měla být v používaném rozsahu.

8.8 Sociální sítě

Sociální sítě se staly fenoménem současné doby. Jak je patrné z obrázku, v současné době jsou cenným zdrojem informací a uživatelů, ale stejně jako jiné druhy internetové komunikace sebou přináší jisté rizika, která by měl každý akceptovat. Jedná se o on-line služby, které umožňují jedincům vystavit svůj veřejný nebo polo-veřejný profil, který pak

slouží k popisu jejich osoby nebo organizace, a zároveň jim umožňuje sestavit si vlastní seznam dalších uživatelů, se kterými je ve spojení. Toto spojení je nejčastěji uskutečněno pomocí např. chatů, zpráv, e-mailů, rychlých zpráv (tzv. instant messages), diskusních skupin apod., které jsou ve většině případů součástí sociální sítě a slouží ke sdílení dat mezi uživateli. Co se týká sdílení dat – jedná se o různé informace v podobě krátkých textových zpráv, povídky, obrazy, fotografie, hudbu až po jiné elektronické soubory.

Obrázek 22 Rozvoj sociálních sítí [46]

8.8.1 Krádež identity prostřednictvím sociálních sítí

První varianta je naprosto banální. Spočívá v uživatelově nepozornosti, tedy tak, že se zapomene ze svého účtu odhlásit (např. knihovna, internetová kavárna, areálová studovna). Kdokoliv další, kdo přijde k počítači tak má neomezené práva disponovat s jeho profilem, Další možností je, že si nejprve útočník vytvoří profil. K jeho vytvoření použije fotografie a jiné údaje nalezené náhodně (častokrát však cíleně) na různých internetových portálech. Jde o řadu osobních často až důvěrných informací, které mají vzbudit dojem, že daný profil je pravý a je za ním je skutečně osoba, jejíž identitu chce zneužít. Po vytvoření takového

profilu s falešnou identitou následuje komunikace s jinými diskutéry na dané sociální síti - obvykle útočná, vulgární, často cílená na dobré jméno skutečného nositele dané identity. Nejčastějším motivem bývá snaha ublížit potenciální oběti - zesměšnit ji, oslabit její postavení v nějaké sociální skupině (v zaměstnání, škole, přátelském kolektivu), v případě organizace poškodit dobré jméno firmy, popř., avšak spektrum potenciálních motivů takového řízení může být mnohem širší. Zásadním problémem je skutečnost, že osoby, jejichž identita je takto zneužita o této skutečnosti ani nevědí a často se to dozvídají náhodně od jiných a obvykle se značným časovým odstupem kdy se podobná komunikace skutečně probíhala.

Nejčastější důvody vytvoření falešné identity:

- Marketing – přední společnosti disponují širokým okruhem uživatelů (např. společnost Škoda auto více než 500 000), což z hlediska marketingu představuje velmi silnou materii.
- Pomluva – může se vztahovat k běžnému uživateli, tak veřejně známé osobnosti.
- Kyberšikana - šikanování jiné osoby pomocí informačních technologií - internetu, mobilních telefonů, apod. (např. vydírání, ubližování, ztrapňování, obtěžování, ohrožování, zastrašování apod.
- Kybergrooming - je termín, který označuje chování uživatelů internetu, které má v dítěti vyvolat falešnou důvěru a připravit ho na schůzku, jejímž cílem je nezletilou/zletilou oběť unést, pohlavně zneužít či jinak poškodit.
- Získání citlivých údajů – nebezpečí získání citlivých údajů uživatelů, ale i vládních složek. Příkladem experiment Thomase Ryana, který vytvořil fiktivní profil dívky, vydávající se za expertku na bezpečnost. Během 2 měsíců získal kontakty na odborníky z oblasti administrátorů, armády a bezpečnostních odborníků. Získání informací probíhalo žádostmi o pracovní nabídky, nabídky na schůzku, přístup k interním informacím, žádosti o odbornou korekturu prací. [45]

Obrázek 23 Fiktivní profil [45]

8.8.2 Obrana proti krádeži identity na sociální síti

Nereagovat. Pouštět se do komunikace nebo vysvětlování v rámci takové diskuse v případě komunikace na internetu nemá žádný pragmatický smysl. Jednak diskutující může sedět na opačném konci světa, jednak komunikaci přihlíží početně neodhadnutelné publikum, ze kterého se s vysokou pravděpodobností při stupňování diskuse vyprofiloval další diskutéři přidávající "zaručené " svědectví o osobě oběti a jeho blízkém okolí .

Zákonná práva a trestní oznámení. V takovém případě jde minimálně o zneužití osobních údajů, čímž autor fiktivního profilu spáchal trestný čin neoprávněného nakládání s osobními údaji, v nemalé míře přichází v úvahu i řadu dalších skutečností, kterými mohla být způsobena nemajetková případně i majetková újma.

Využití dostupné možnosti na zrušení takového profilu včetně diskuse. Mnoho sítí má dnes velmi jednoduché postupy na ohlášení takového zjištění.

8.9 Keylogger

Tento pojem by šel do češtiny přeložit jako odposlech klávesnice. Může být prováděn dvojím způsobem. První variantou je nainstalování programu (např. Freekeylogger, ActivityMon, Safetica), které slouží k uchování všech hesel, které uživatel zadá. Pachatel tak může využít volně přístupných prostor jako například internetové kavárny, knihovny či areálové studovny a poté provést „sběr“ shromážděných dat.

Druhou variantou je odposlech pomocí elektromagnetických vln. Ty jsou vyzařovány z klávesnice (nezáleží na druhu připojení, mění se jen intenzita vyzařování) při stisku jednotlivých kláves. Dekódovací software pak přiřadí k jednotlivým pulzům znaky. Byly provedeny měření, které na vzdálenost 20m dokázaly dekódovat 95% znaků. Aktivní ochrana proti tomuto způsobu trestné činnosti je zavedení tzv. virtuálních klávesnic, které již dnes využívají všechny banky. [15]

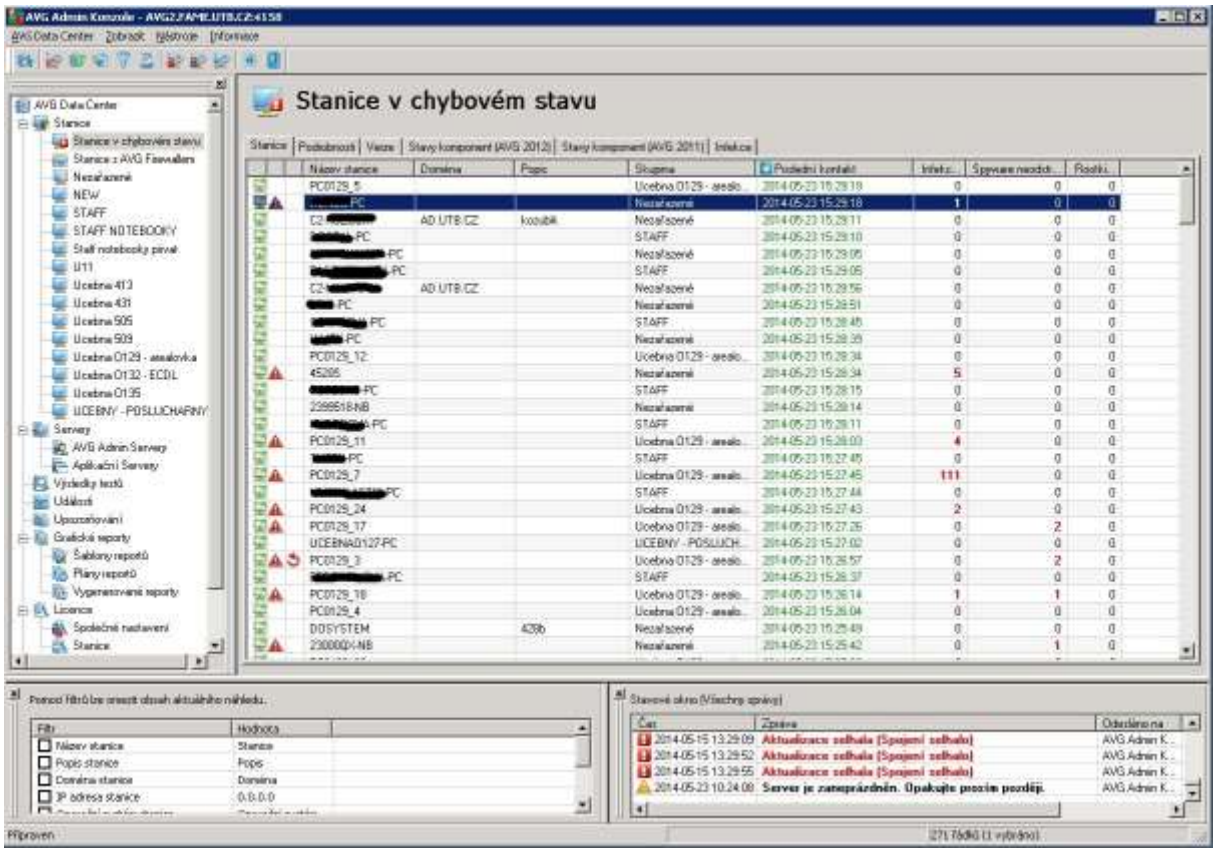
Obrázek 24 Virtuální klávesnice [47]

8.10 Nigérijské dopisy

Jedná se o řetězový e-mail, který požaduje pomoc pro nemocného, opuštěná zvířata, nebo jakékoliv jiné způsoby zkonstruované pro apelování na smysly čtenáře. Ale tyto e - maily nejsou ničím jiným než formou podvodu. Tyto dopisy mají formu e - mailu informujícího příjemce, že vyhrál loterii nebo slosování nebo žádající o pomoc při vyhnutí se dani z příjmu za značnou odměnu. Ve skutečnosti se pokouší podvést uživatele, která je pak požádán o zaslání určitého množství peněz pro zaplacení celních poplatků, spotřebních daní, odměny úředníkům apod. [15]

8.11 Situace bezpečnostních incidentů v síti FaME

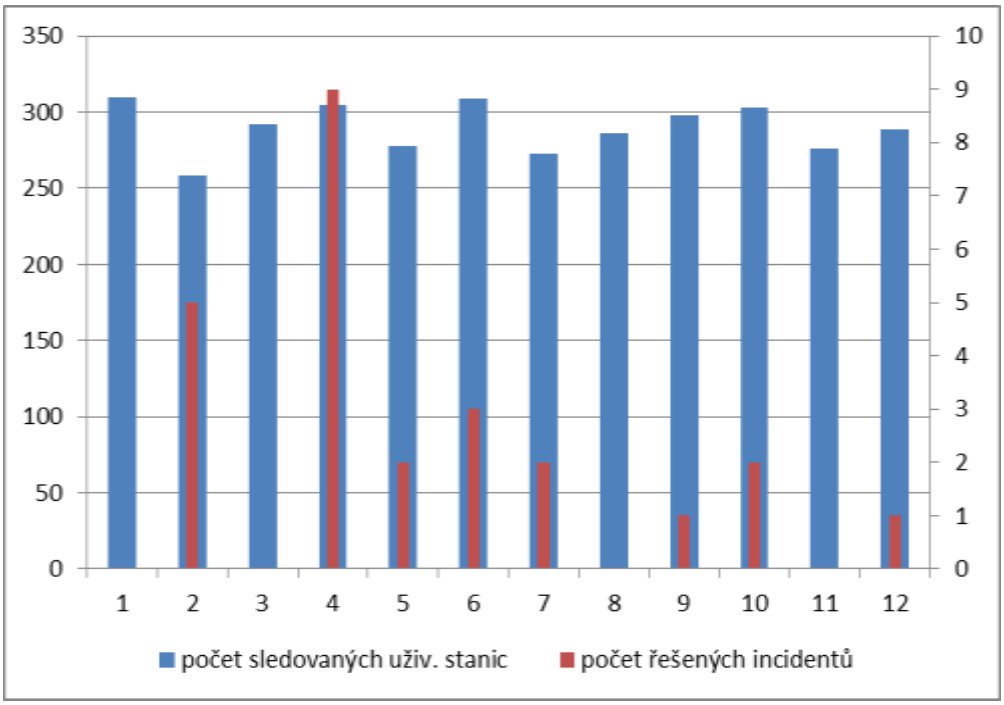
Tato kapitola se věnuje situaci phishingových útoků, konkrétně v univerzitní síti FaME. Zdrojem dat je administrátorská konzole AVG, která slouží ke vzdálené správě uživatelských stanic. Pomocí konzole má správce kompletní přehled nad bezpečnostními incidenty v síti, tvorba reportů, řízení aktualizací, konfiguraci událostí nebo změnu licenčního čísla.



Data byla sledována v rozmezí od 1. 9. 2013 do 31. 5. 2014. Graf znázorňuje stav bezpečnostních incidentů ve sledovaném prostředí.

Tabulka 3 Stav bezpečnostních incidentů

číslo	datum incidentu	počet sledovaných uživ. stanic	počet řešených incidentů	typ incidentu	použité řešení nad rámec standartních postupů
1	15.9.2013	310	0	phishing na bankovní účet	varovný e-mail
2	10.10.2013	258	5	trojský kůň	varovný e-mail
3	17.10.2013	292	0	trojský kůň	
4	1.11.2013	305	9	pharming	blokace IP adres, nahlášení nevhodného odkazu
5	19.11.2013	278	2	pharming	blokace IP adres
6	12.12.2013	309	3	phishing na e-mailový účet	
7	20.12.2013	273	2	trojský kůň	
8	14.2.2014	286	0	pharming	blokace IP adres
9	2.3.2014	298	1	pharming	blokace IP adres, nahlášení nevhodného odkazu
10	17.3.2014	303	2	phishing na e-mailový účet	
11	28.4.2014	276	0	phishing na bankovní účet	varovný e-mail
12	13.5.2014	289	1	phishing na e-mailový účet	



Obrázek 25 Zpracovaná data [vlastní]

9 ORGANIZOVANÝ ZLOČIN V OBLASTI KRÁDEŽE IDENTITY

9.1 Typy hackerů

Zpravidla se jedná o skupinu lidí, která pro peníze či s cílem obecně škodit provádí nejrůznější aktivity. Například může jít o rozesílání nevyžádaných e-mailů, nebo distribuci malware. Do počítačů běžných uživatelů internetu se tak mohou dostat spamy s nejrůznějším obsahem včetně virů a trojských koní. Ty pak škodí a samovolně se aktivují v uživatelově počítači. Vzhledem k tomu, že internet nezná hranice, pochází tyto skupiny z různých koutů světa – převážně ze zemí bývalého Sovětského svazu, Číny, ale také z amerického kontinentu.V tabulce je znázorněna kategorizace hackerů. [39]

Tabulka 4 Pachatelé kybernetické kriminality [vlastní]

Kiddiots / script Kiddies	Jsou na nejnižší úrovni v páchání této trestné činnosti. Dokážou nalézt na internetu kód a upravit jej pro spuštění nové varianty viru.
Tvůrce virů	Lépe ovládá programování na vyšší úrovni. Píše viry a zveřejňuje je na internetu nebo dokáže spustit virový útok elektronickou poštou.
Příležitostný hacker	Tvůrce virů se zapojuje do světa elektronického zločinu. Pracuje většinou jako programátor či v oboru informačních technologií.
Profesionální hacker	Ten se živí krádežemi kreditních karet, změnou webových stránek, či dokonce elektronickým vydíráním.
Phisher	Vytváří falešné webové stránky, ze kterých získává hesla pomocí metod sociálního inženýrství. Podvodem pak získává velké částky peněz z účtu.
Nájemný počítačový pachatel kybernetické kriminality	Ten nabízí své znalosti tomu, kdo nabídne nejvyšší cenu za jeho služby.

9.2 Problematika hesel

Počítačová hesla jsou na každém našem elektronickém kroku. Jedná se například o hesla pro přihlášení k počítači, e-mailu, wifi síti, elektronickému obchodu, na různá diskuzní fóra nebo Facebook. Používání jednoho hesla k přihlášení na všechny služby, které uživatel používá, není bezpečné. Pokud totiž někdo získá tajné heslo, může zneužít identitu a může

praktikovat různé činnosti, které souvisí se vstupem do e-mailového účtu., stahovat osobní data, nakupovat v e-shopech, a to vše jménem podvedeného.

Mnoho lidí se dopouští základní chyby – používá stejné heslo pro více účtů. Útočníkům potom stačí hacknout jeden účet a rázem mají přístup i k těm ostatním. Většina služeb se váže na email a na něj jsou i zasílána hesla, potvrzení o jejich změně, ověření a podobně. Je tedy zřejmé, že emailová schránka je důležitou komoditou a také tím prvním, co se případný zájemce o prolomení pokusí napadnout. V tabulce níže, jsou uvedeny nejčastěji používaná hesla za loňský rok. [48]

Tabulka 5 Nejpoužívanější hesla [48]

Pořadí	Heslo
1	123456
2	password
3	12345678
4	qwerty
5	abc123
6	123456789
7	111111
8	1234567
9	trustno1
10	adobe123

9.2.1 Lámání hesel

Útoky na heslo jsou velice starou metodou, která je ale pořád aktuální. Mnoho uživatelů používá jednoduchá hesla, která se nějakým způsobem snaží útočník získat. Takových způsobů je více, nejčastější metoda lámání hesel.

Nástroje na hádání hesel patří k prvně používaným hackerským nástrojům, tzv. password crackers a slouží k prolomení ochrany nebo autorizace, která je zabezpečena statickým heslem. Pracují tak, že zkouší nejrůznější kombinace znaků, pokud heslo projde autorizací, odešle jej útočníkovi. Útok tímto nástrojem je dvojího druhu a rozdíl je v tom, jak zkouší kombinace znaků:

- Slovníkové útoky (dictionary attack) – zkouší použít známá hesla z vlastní databáze slov.

- Útok hrubou silou (brute-force attack) – zkouší postupně všechny možné kombinace hesla s potřebnou délkou z vybraných znaků

V tabulce níže jsou uvedeny časové údaje vybraných délek hesel. Pro údaje v tabulce předpokládáme, že útok je veden z jednoho počítače a rychlost útoku je 500 000 hesel za vteřinu. Jsou zde uvedeny nejzazší termíny prolomení hesla. [48]

Tabulka 6 Lámání hesel [49]

Délka hesla	Sada znaků			
	Malá písmena	Malá písmena a číslice	Malá a velká písmena	Všechny ASCII znaky
< = 4	okamžitě			2 minuty
5	okamžitě	2 minuty	12 minut	4 hodiny
6	10 minut	72 minut	10 hodin	18 dní
7	4 hodiny	43 hodin	23 dní	4 roky
8	4 dny	65 dní	3 roky	463 let
9	4 měsíce	6 let	178 let	44530 let

9.2.2 Autorizační sms

Jedná se o způsob ověření, kdy banka při požadavcích o autorizaci zašle klientovi SMS s potvrzovacím kódem, který je potřeba opsat zpět do aplikace. Jedná se o velmi bezpečnou metodu, která má ovšem také svá omezení. Součástí SMS bývá často také informace o tom, k čemu se konkrétní kód vztahuje. Pokud uživatel tyto informace nekontroluje, je poměrně snadné mu podvrhnout falešnou webovou stránku a provést úplně jiný krok než ten, který uživatel očekává. Některé banky navíc žádné podrobné informace ve zprávách nezasílají, takže je není podle čeho ověřit.

Podvod, kterým se útočník snaží získat SMS kód, probíhá zpravidla pomocí:

a) podvržené stránky, do které je uživatel vyzván k doplnění kódu potřebného k autorizaci.

Obrázek 26 Falešná stránka pro zisk autorizačního kódu [50]

b) autorizační SMS pomocí sociálního inženýrství, která spočívá v důvěřivosti klamané osoby. Probíhá tak, že pachatel ji kontaktuje buď pomocí SMS nebo telefonního hovoru a žádá o zaslání autorizačních údajů. Ač to zní nereálně, tyto případy se opravdu stávají poměrně často.

10 ODHAD DALŠÍHO VÝVOJE

Odhad dalšího vývoje je závislý na mnoha okolnostech, protože zasahuje do oblasti technických, kulturních, politických a personálních rovin. Co se týče sociální identity, která je charakterizována především fyzickými doklady, situace spojená s pácháním trestných činů nebude nijak narůstat, naopak bude probíhat každoroční mírný pokles. V problematice virtuálních identit je situace diametrálně odlišná. Je závislá především na vývoji nových technologií a na jejich rozšíření mezi uživatele. Značným rozvojem prošel za posledních několik let vývoj mobilních telefonů. Nyní jsou nejen zdrojem důležitých dat a informací, ale se zavedením technologie NFC se staly i jakousi náhradou platební karty což jen zvyšuje riziko jejich krádeže nebo jiné nekalé činnosti. Zatím tuto službu podporuje pouze jeden mobilní operátor, do budoucna je očekávána nabídka stejné služby i od ostatních a tak i zvýšení počtu uživatelů aplikace.

Obrázek 27 Telefon s technologií NFC [51]

10.1 QR kódy

Čím dál častěji se hrozbou stávají také QR kódy, které byly dříve doménou několika nadšenců, ale dnes je zná celý svět. Objevuje se jich čím dál více, lidé si na ně začínají zvykat a běžně je používají. Jedná se přitom o efektivní metodu, jak napadnout uživatele. Stačí si vytvořit nebezpečnou stránku a přelepit QR kódy třeba na reklamách v metru.

Obrázek 28 QR kódy [51]

10.2 Win XP

Softwarová firma Microsoft ukončí podporu operačního systému Windows XP 8. dubna 2014. To znamená, že nově zjištěné chyby nebudou opravovány, takže systémy v různých částech světa budou zranitelné. Předpokládám, že hackeři, kteří již mají exploity, budou útočit s cílem prodat je v nejvyšší nabídce. Vzhledem k očekávané vysoké ceně je pravděpodobné, že tyto zranitelnosti budou spíše využity k zahájení cílených útoků proti firmám s vysokou hodnotou a bohatým jednotlivcům, než k nasazení u běžných počítačových útočníků k šíření masové infekce.

10.3 Využití biometrických údajů

Letos Apple udělal odvážný krok, když oznámil, že jeho nový iPhone 5s bude mít integrovaný otisk prstu jako autentizaci uživatele pro přístup do přístroje. Není důležité, že byl hacknutý (hacked) jen několik dní po jeho uvedení na trh, lidi to přinutilo mluvit

o významu dvou faktorové autentizace (two-factor authentication) ve světě, kde se jednoduché přihlašování pomocí hesla stává stále větším archaismem. V důsledku tohoto obnoveného zájmu předpokládám, že příští rok přidají druhý faktor autentizace do svých zařízení další mobilní výrobci. Budeme také svědky nárůstu dalších forem ověřování, jako je skenování duhovky nebo rozpoznání obličeje.

ZÁVĚR

Závěrem práce bych zrekapituloval prezentované informace. Problematika krádeží identit se dotýká lidské existence už od pradávna. S časem a vývojem nových technologií v oblasti identifikace osob se měnila pouze v závislosti na dovednostech, prostředcích, popř. finančním zázemí pachatele.

Oblast krádeže identity jsem rozdělil na dvě odvětví. První, které je definováno jako sociální identita, zahrnuje prostředky k prokázání totožnosti v podobě osobních dokladů, ale také dalších citlivých údajů, podle nichž můžeme osobu jednoznačně identifikovat. Jedním z nich je také platební karta, které jsem díky jejímu rozšíření a možnostem věnoval zvláštní pozornost. Dnes již totiž jen velmi těžko najdeme člověka, který by nedisponoval alespoň jednou platební kartou, k níž bývá zpravidla zřízen běžný bankovní účet. Spojení těchto dvou aspektů otevírá majiteli nové možnosti ke správě svých finančních prostředků, ale zároveň také nese riziko možného zneužití, a to ať už krádeží karty nebo za použití identifikátorů potřebných k internetovému bankovnictví.

Druhé odvětví je spjato s prudkým rozvojem internetu a rozvojem nových technologiích, která jsou na jejich možnostech přímo závislé. Jde především o rozvoj elektronického bankovnictví, přístup do webových portálů, sociálních sítí a jiných komunikátorů. Tato oblast je v práci definována jako virtuální identita.

V práci jsem se zaměřil především na bezpečnost z pohledu uživatele. Technické řešení ze strany institucí lze považovat za poměrně dobře zpracované a tak se pachatelé trestné činnosti spjaté s citlivými daty a finančními prostředky zaměřují na koncové uživatele. Ti mnohdy slepě uvěří jakýchkoliv výzev útočníků k odeslání citlivých údajů, nebo přímo finanční hotovosti. Je tedy zřejmé, že na problematiku bezpečnosti lze obecně nahlížet ze dvou stran. Vedle sebe stojí technický aspekt a lidský faktor. Oba jdou ruku v ruce, a pokud klopýtá jeden z nich, objevuje se potenciální riziko. Uživatelský přístup je otázkou konkrétní informovanosti, zodpovědnosti a údržby počítače, přes který klient přistupuje do různých internetových služeb.

Cílem diplomové práce bylo přiblížit možnosti, jakými způsoby je možné realizovat útoky na lidskou identitu, charakterizovat je a provést možná protiopatření, která by minimalizovaly jejich dopady. Tyto metody, návrhy a postupy jsou součástí praktické části.

Věřím, že tato práce poskytne čtenáři kompletní přehled o dané problematice a ozřejmí mu důvody preventivních opatření, které jsem v této práci prezentoval.

SEZNAM POUŽITÉ LITERATURY

Bibliografie

[20] JIROVSKÝ, Václav. Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Redaktor Martin Kysela. 1. vyd. Praha : Grada Publishing, 2007. 288 s. ISBN 978-80-247-1561-2.

[32] Matoušová, M., Hejlík, L. (2008, 2. dopl. a aktualiz. vyd.). Osobní údaje a jejich ochrana. Praha: Aspi. ISBN 978-80-7357-322-5.

[33] RAK, Roman. *Biometrie a identita člověka ve forenzních a komerčních aplikacích: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2008, 631 s., 32 s. barev. obr. příl

[37] LANCE, James, Lubomír DLOUHÝ. *Phishing bez záhad*. Praha: Grada, 2007. ISBN 80-247-1766-2.

[38] JAŠEK, Roman. *Informační a datová bezpečnost*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. ISBN 80-7318-456-7.

[39] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství Aleš Čeněk, 2005.

Internetové zdroje

[1] SCHEINOST, PhDr. Miroslav a JUDr.Zdeněk KARABEC,CSC. Zneužití identity a trestná činnost s tím spojená. *Ministerstvo vnitra ČR* [online]. [cit. 2014-05-24]. Dostupné z: www.mvcr.cz/soubor/scheinostkarab-identity-pdf.aspx

[2] Ukradená identita. *Www.lidovky.cz* [online]. [cit. 2014-05-24]. Dostupné z: http://www.lidovky.cz/boom-kradezi-identity-kazdy-druhy-den-resi-policie-novy-pripad-p7h-/zpravy-domov.aspx?c=A130416_215427_ln_domov_ml

[3] Online krádeže citlivých údajů. *Www.lupa.cz* [online]. [cit. 2014-05-24]. Dostupné z: http://www.lupa.cz/clanky/online-kradeze-citlivych-udaju-dobry-byznys-pro-hackery/

[4] Elektronický podpis. *Bezpečnost informačních systémů* [online]. 2011 [cit. 2014-05-24]. Dostupné z: http://czdva.webnode.cz/ochrana/kryptografie/elektronicky-podpis/

[5] Co je elektronický podpis. *Bezpečnost informačních systémů* [online]. 2011 [cit. 2014-05-24]. Dostupné z: http://www.ica.cz/Elektronicky-podpis

[6] Co jsou digitální certifikáty. *Bussiness communication* [online]. 2009 [cit. 2014-05-24]. Dostupné z: http://www.certifikaty.com/certifikaty/co-jsou-digitalni-certifikaty

[7] Šifrování SSL. *Česká spořitelna* [online]. 2014 [cit. 2014-05-24]. Dostupné z: www.csas.cz

[8] Definice pojmů. *Úřad na ochranu osobních dokladů* [online]. 2013 [cit. 2014-05-24]. Dostupné z: http://www.uoou.cz/slovnicek-nejdulezitejsich-pojmu/ds-2617/p1=2617

[9] Občanské průkazy, cestovní pasy a rodné čísla. Západočeská univerzita [online]. 2012 [cit. 2014-05-24]. Dostupné z: https://otik.uk.zcu.cz/bitstream/handle/11025/8310/Obcanske%20prukazy,%20cestovni%20doklady%20a%20rodna%20cisla.pdf?sequence=1

[10] Osobní doklady. *Ministerstvo vnitra ČR* [online]. 2014 [cit. 2014-05-24]. Dostupné z: www.mvcr.cz/clanek/osobni-doklady.aspx

[11] Osobní doklady. *Státní správa* [online]. 2014 [cit. 2014-05-24]. Dostupné z: http://www.statnisprava.cz/rstsp/redakce.nsf/i/vnitro

[12] Elektronická identifikace občana. *Estat* [online]. 2012 [cit. 2014-05-24]. Dostupné z: http://www.estat.cz/data/publikace_karel_neuwirt_1.pdf

[13] Skimming. *Policie ČR* [online]. 2012 [cit. 2014-05-24]. Dostupné z: www.policie.cz/clanek/skimming-2011.aspx

[14] *Karty s magnetickým pruhem* [online]. 2008 [cit. 2012-05-17]. ISSN 1803-6007. Dostupné z: http://pandatron.cz/?535&karty_s_magnetickym_pruhem

[15] Portal UTB. *Portál UTB* [online]. 2012 [cit. 2014-05-24]. Dostupné z: http://portal.utb.cz/zaverecneprace/hubacekpavel

[16] *Příručka držitele karty* [online]. 2011 [cit. 2014-05-20]. Dostupné z: http://www.csas.cz/banka/content/inet/internet/cs/Prirucka_drzitele_PK.pdf

[17] EHIC. *Zdravotní pojišťovna ministerstva vnitra* [online]. 2014 [cit. 2014-05-24]. Dostupné z: http://www.zpmvcr.cz/lekari/prukazy-zdravotniho-pojisteni/evropsky-prukaz-ehic1/

[18] Corpus solutions. *Budoucnost zcizení a krádeže identity* [online]. 2010 [cit. 2014-05-24]. Dostupné z: http://www.corpus.cz/cs/o-spolecnosti/tiskove-centrum/napsali-o-nas/t184.html

[19] Online krádeže citlivých údajů: dobrý byznys pro hackery. *Lupa.cz* [online]. 2007 [cit. 2014-05-24]. Dostupné z: Online krádeže citlivých údajů: dobrý byznys pro hackery

[21] *Československá obchodní banka* [online]. 2012 [cit. 2014-05-25]. Dostupné z: http://www.csob.cz/cz/Csob/Servis-pro-media/Tiskove-zpravy/Stranky/TZ120801.aspx

[22] A Portrait of J. Random Hacker [online]. 2012 [cit. 2014-05-25]. Dostupné z: http://project.cyberpunk.ru/idb/portrait_of_j_random_hacker.html]

[23] *Portál veřejné správy* [online]. 2014 [cit. 2014-05-25]. Dostupné z: http://portal.gov.cz/app/zakony/

[24] Institut pro kriminologii a sociální prevenci. KONGRES OSN O PREVENCI KRIMINALITY. *KONGRES OSN O PREVENCI KRIMINALITY* [online]. 2005 [cit. 2014-05-25]. Dostupné z: http://www.ok.cz/iksp/docs/322.pdf

[25] Idnes.cz. *Česko zasáhly krádeže identity* [online]. 2012 [cit. 2014-05-25]. Dostupné z: http://ekonomika.idnes.cz/cesko-zasahly-kradeze-identit-dkl-/ekonomika.aspx?c=A120504_085107_ekonomika_neh

[25] Úřad na ochranu osobních údajů. *Česko zasáhly krádeže identity* [online]. 2004 [cit. 2014-05-25]. Dostupné z: http://www.uoou.cz/ukradeny-prukaz-klic-k-podvodum/ds-2025/p1=2025

[26] Skimming. *Http://www.policie.cz/clanek/skimming.aspx* [online]. 2012 [cit. 2014-05-25]. Dostupné z: http://www.policie.cz/clanek/skimming.aspx

[27] *Skimming* [online]. 2010-2014 [cit. 2014-05-20]. Dostupné z: http://www.cybersecurity.cz/data/skimming.pdf

[28] *Alibaba* [online]. 1999-2014 [cit. 2012-05-25]. Dostupné z: http://www.alibaba.com/trade/search?Country=&IndexArea=product_en&fsb=y&SearchText=card+reader+skimmer

[29] Česká společnost pro systémovou integraci. *Soudobé trendy v oblasti mobilních zařízení* [online]. 2013 [cit. 2014-05-25]. Dostupné z: www.cssi.cz/cssi/system/files/all/SI_2013_2_05_Oganesjan.pdf

[30] Policie ČR. *Krádež identity* [online]. 2013 [cit. 2014-05-24]. Dostupné z: http://www.policie.cz/clanek/ztrata-identity.aspx

[31] Česká společnost pro systémovou integraci. *Soudobé trendy v oblasti mobilních zařízení* [online]. 2013 [cit. 2014-05-25]. Dostupné z: www.cssi.cz/cssi/system/files/all/SI_2013_2_05_Oganesjan.pdf

[34] Bankovnictví. *Jak se bránit zneužití dokladů a finanční ztrátě* [online]. 2013 [cit. 2014-05-25]. Dostupné z: http://bankovnictvi.ihned.cz/c1-16460760-jak-se-branit-zneuziti-dokladu-a-financni-ztrate

[35] .Eamos *Trojské koně* [online]. 2002-2014 [cit. 2014-05-25]. Dostupné z: http://eamos.pf.jcu.cz/amos/kat_inf/modules/low/kurz_text.php?id_kap=9&kod_kurzu=kat_inf_52453

[36] Phishing. *Co je phishing* [online]. 2012 [cit. 2014-05-25]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing [37]

[40] Firewall. *Antivirové centrum* [online]. 2012 [cit. 2014-05-25]. Dostupné z: http://www.antivirovecentrum.cz/firewally.aspx

[41] Bezpečný internet [online]. 2008-2010 [cit. 2014-05-20]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx

[42] ITBIZ. *Phishing a další formy útoků* [online]. 2008 [cit. 2014-05-25]. Dostupné z: http://www.itbiz.cz/phishing-check-point

[43] Pharming může ošálit i zkušenějšího uživatele internetu. *Ihned.cz* [online]. 2008 [cit. 2014-05-25]. Dostupné z: http://tech.ihned.cz/c1-23480750-pharming-muze-osalit-i-zkusenejsiho-uzivatele-internetu

[44] Spoofing. *Spoofing* [online]. 2008 [cit. 2014-05-25]. Dostupné z: http://spoofing.cz/

[45] Policie ČR. *O kybešikaně* [online]. 2012 [cit. 2014-05-25]. Dostupné z: http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

[46] Bezpečnostní seminář. *Lynuxexpress* [online]. 2014 [cit. 2014-05-25]. Dostupné z: http://www.linuxexpres.cz/seminar-bezpecny-provoz-siti-a-sluzeb-od-sdruzeni-cesnet

[47] Česká spořitelna. *Virtuální klávesnice* [online]. 2014 [cit. 2014-05-25]. Dostupné z: www.csas.cz

[48] Nejhorší hesla 2013. *Zive.cz* [online]. 2014 [cit. 2014-05-25]. Dostupné z: http://www.zive.cz/bleskovky/25-nejhorsich-hesel-roku-2013-adobe-zamichalo-poradim/sc-4-a-172164/default.aspx

[49] Bruteforce attack. *KitLab laboratorní server* [online]. 2014 [cit. 2014-05-25]. Dostupné z: http://kitlab.pef.czu.cz/~lohr/wiki/index.php/Bruteforce_attack

[50] Zneužití internetového bankovnictví skrze SMS. *Patria online* [online]. 2014 [cit. 2014-05-25]. Dostupné z: http://www.patria.cz/zpravodajstvi/2131715/ceska-sporitelna-odhalila-novy-zpusob-zneuziti-internetoveho-bankovnictvi-skrze-sms.html

[51] Chip. *Hrozby 2014* [online]. 2013 [cit. 2014-05-25]. Dostupné z: http://www.chip.cz/novinky/top-5-nejvetsich-bezpecnostnich-trendu-pro-rok-2014/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CA	Certifikační autorita
ČR	Česká republika
DNS	Systém doménový jmen (Domain Name Server)
HTTP	Hypertextový protokol (HyperText Transfer Protokol)
NFC	Near Field Communication
PIN	Bezpečnostní kód (Personal Identification Number)
RFID	Technologie bezdrátové komunkace (Radio Frequency Identification)
SIM	Čip mobilního telefonu (Subscriber Information Module)
SSL	Bezpečnostní vrstva (Secure Socket Layer)
SMS	Krátké textové zprávy (Short Message Service)
HTTPS	Hypertext Transfer Protocol Secure
URL	Uniform Resource Locator
ČSÚ	Český statistický úřad
ICQ	Hypertext Transfer Protocol Secure
CVV	Card verification value
USA	United States of America (Spojené státy americké)
MPSV	Ministerstvo práce a sociálních věcí
FaME	Fakulta managementu a ekonomiky

SEZNAM OBRÁZKŮ

SEZNAM TABULEK