



EVROPSKÁ DOKUMENTACE O POTÍRÁNÍ PODVODŮ PŘI BEZHOTOVOSTNÍCH PLATBÁCH

***Jak se můžete chránit
proti různým druhům podvodů?***

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author,
and the Commission cannot be held responsible for any use which may be
made of the information contained therein



Všeobecná situace a rozsah metod bezhotovostních plateb a podvodů

Pokrok globálních metod bezhotovostních plateb je nesporný. Karty, převody, šeky, nové prostředky platby po internetu, platby mobilním telefonem a další jsou k dispozici všem uživatelům. Podle "World Payments Report 2008" (Světové zprávy o platbebních prostředcích 2008) provedené společností Capgemini (Royal Bank of Scotland (RBS) a European Financial Management and Marketing Association (EFMA)) představují karty 54% celosvětového objemu plateb. Tento způsob platby je na druhém místě za hotovostním prostředkem s ročním růstem mezi roky 2001 a 2006 16% celosvětově a 11% v Evropě. Elektronické platební transakce rovněž zaznamenaly výrazný vzrůst s přibližně 210.000 miliony transakcí na celém světě. Když používáme takové způsoby plateb, jsme si však vědomi všech rizik, kterým jsme vystaveni? Známe svá práva? Víme na příklad, že instituce nabízející tyto způsoby plateb může být zproštěna odpovědnosti v případě podvodu?

Spotřebitelské organizace v několika zemích EU se účastní na realizaci evropského projektu s cílem čelit situaci a konstruktivně přispět k jejímu řešení. Kooordinátorem realizace projektu je ADICAE, jediná španělská spotřebitelská organizace specializující se na banky, spořitelny a pojišťovací společnosti; partnerem realizace v ČR je Sdružení českých spotřebitelů, o.s. (SČS).

Cílem projektu je dokumentovat podvody a takovouto bázi poskytnout k dispozici nejen spotřebitelům, ale i např. soudním a policejním orgánům a dalším zainteresovaným osobám; byla by založena na varování a informacích poskytnutých finančními institucemi a občany, s cílem informovat a varovat uživatele o rizicích spojených s užíváním těchto platebních postupů a podporovat jejich správné používání, aby se zabránilo podvodům, což je v současnosti hlavním cílem. Jedním z výstupů projektu je tato publikace o podvodech, která chce poskytnout přehlednou formou informace o situaci v podvodných praktikách a obrany proti nim.



Do projektu jsou zapojena kromě Španělska a ČR zapojen spotřebitelská sdružení z Itálie, Litvy, Rumunska, Slovenska a Slovinska.



SCS

web: <http://www.konzument.cz/>



FEDERCONSUMATORI

web: www.federconsumatori.it



LNCF

web: <http://vartotojai.eu/>



ANPCPPS

web: <http://www.anpcpps.ro/>



ASC

web: <http://www.zss.sk/>



MIPOR

web: <http://www.mipor.si/>

2. Současná situace platebních prostředků v Evropské unii



2.1. Úvod

V eurozóně je současně v oběhu více než 350 milionů karet, které se používají pro více než 12 bilionů platebních transakcí a 6 bilionů vyzvednutí peněz v hotovosti každým rokem.

Evropský trh pro bezhotovostní prostředky plateb stále roste. V Evropě bylo provedeno v roce 2006 celkem 70 bilionů různých hotovostních transakcí, ekvivalent rovný jedné třetině globálního trhu. Země eurozóny odpovídají za téměř 73% celkového objemu, s pěti zeměmi odpovídajícími za 85% všech transakcí v eurozóně. (...). Existují dva všeobecné trendy:

- 1 Karty jsou hlavním způsobem platby jiným než v hotovosti se stálou rychlostí vzrůstu 11% za rok mezi roky 2001 a 2006.
- 2 Používání šeků klesá, ačkoliv neexistuje ještě skutečná alternativa pro některé druhy plateb P2P (transakce mezi uživateli, např. Ebay).



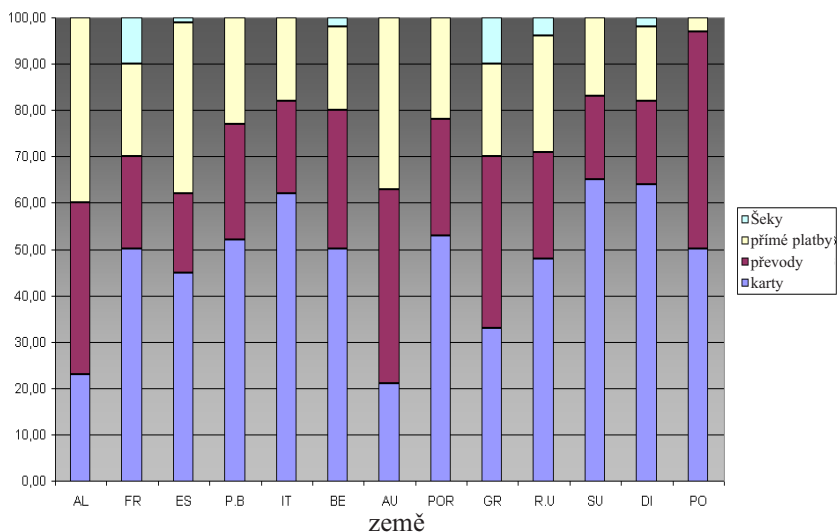


2.2. Statistika

2.2.1. Vzrůst množství transakcí prostřednictvím bezhotovostních plateb

Jak lze vidět v následujícím grafu převzatém z "World Payments Report 2008", pět zemí v eurozóně: Francie, Německo, Holandsko, Španělsko a Itálie odpovídá za 63% všech transakcí s bezhotovostními platbami z celkově vybraných 17 zemí, a 85% všech bezhotovostních transakcí provedených v eurozóně. Tři největší a nejvyspělejší trhy v Evropě jsou: Velká Británie, Německo a Francie.

Odhad použití různých platebních prostředků



Používání bezhotovostních plateb vzrůstá ve všech zemích, ale různými rychlostmi. Případ od případu některé země s vysokým objemem transakcí dosud prožívají významný vzrůst (Německo na příklad mělo kontinuální vzrůst 7% mezi roky 2001 a 2006), zatímco některé země s nízkým objemem transakcí (jako Itálie a Portugalsko) dosud prožívají malé rychlosti vzrůstu.

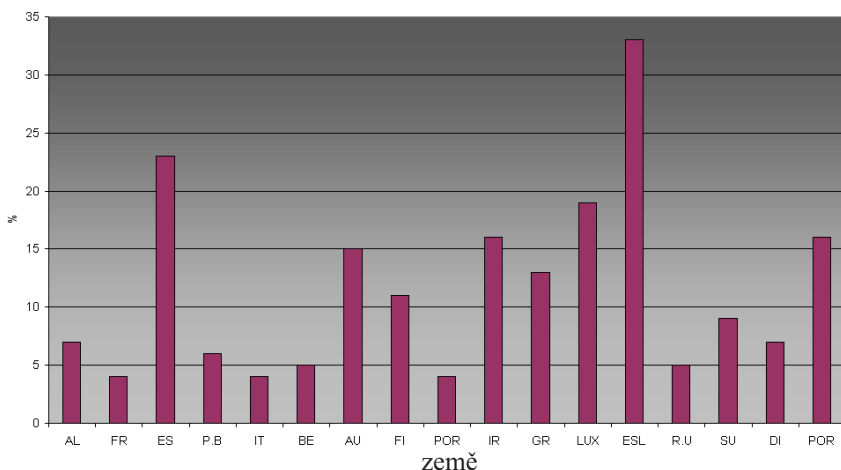


2.2.2. Budoucnost metod plateb v Evropské unii

Na základě výše zmíněné zprávy můžeme předpovědět, jakou budoucnost lze očekávat u bezhotovostních metod plateb. Přetrvávají následující aspekty:

- Systém plateb v Evropě se bude nadále vyvíjet, očekává se všeobecný vzrůst.
- Za předpokladu, že SEPA (the Single European Payments Area) vynaloží značné úsilí na konvergenci bezhotovostních plateb, měl by počet transakcí na občana vzrůstat rychlostí 9 % do roku 2013. Zejména ty země, kde počet transakcí na hlavu byl v roce 2006 menší než 150, by mohly do roku 2013 až zdvojnásobit využívání bezhotovostních platebních prostředků.
- Používání karet by rovněž mělo významně vzrůst, jak poroste počet podniků akceptujících karty, jakož i množství prodávaných výrobků. To by bylo zejména pozitivní, jestliže relativní používání karet se více rozšíří v zemích jako Itálie, Polsko a Řecko, kde současné používání karet na hlavu je malé.

Průměrné nárůsty počtu transakcí provedených bezhotovostními platebními prostředky (2001-2006)





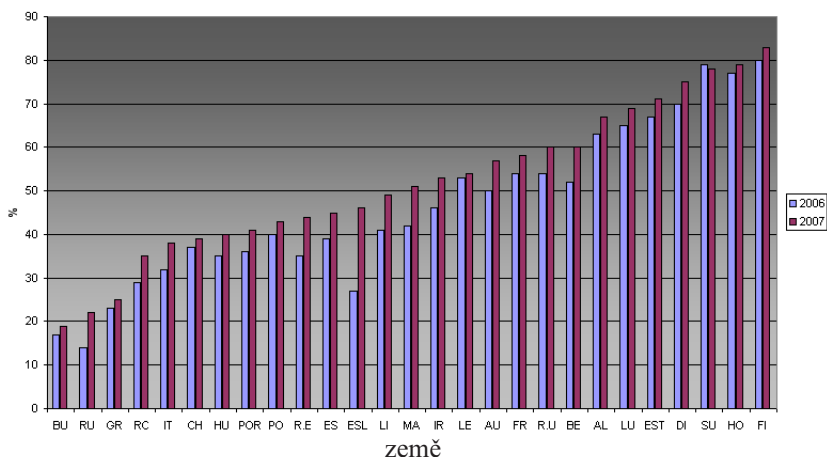
- Ve dvou zemích nejvíce vydávajících šeky, ve Velké Británii a Francii, by měl rozsah způsobů plateb nadále vzrůstat, aby umožnil přechod z šeků na bankovní převody, karty a bezhotovostní platby.

2.2.3. Internetové a elektronické bankovníctví v Evropě

Za poslední roky vzrostl ve větším nebo menším rozsahu počet připojení internetu v domácnostech ve všech zemích evropské unie. V zemích EU15 procentuální podíl domácností s přístupem k internetu činil 59 % (2007), což činí 5 % roční nárůst. Číslo pro všech 27 zemí EU činí 54 % v roce 2007.

Množství lidí používajících elektronické bankovníctví v Evropě narůstá (např. podíl bankovníctví online vzrostl v 27 zemích EU ze 16 % v roce 2004 na 24 % v roce 2007). Jestliže tento trend bude pokračovat, vedlo by to k podílům 50-60 % v roce 2020, tj. úrovni, které je běžná v severských zemích a BENELUXU (údaje z Deutsche Bank, 2008). Podíl osob používajících elektronické bankovníctví velmi závisí na geografickém umístění uživatele.

Uživatelé elektronického bankovníctví

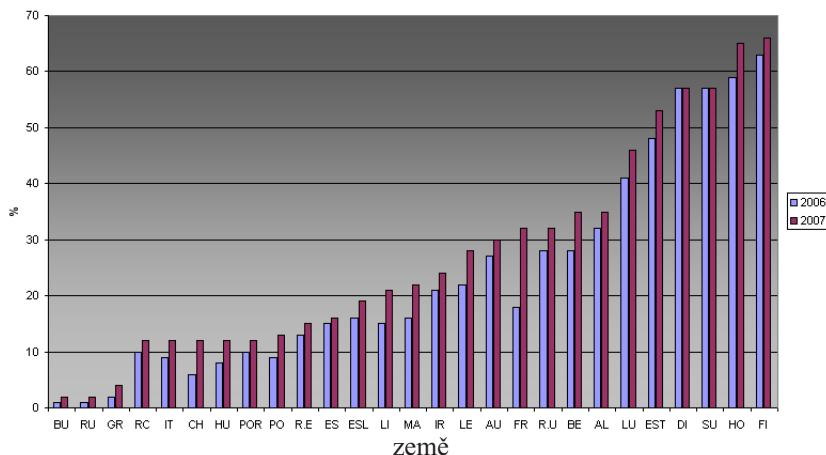




2.2.4. Informace týkající se podvodů při různých formách platebních prostředků

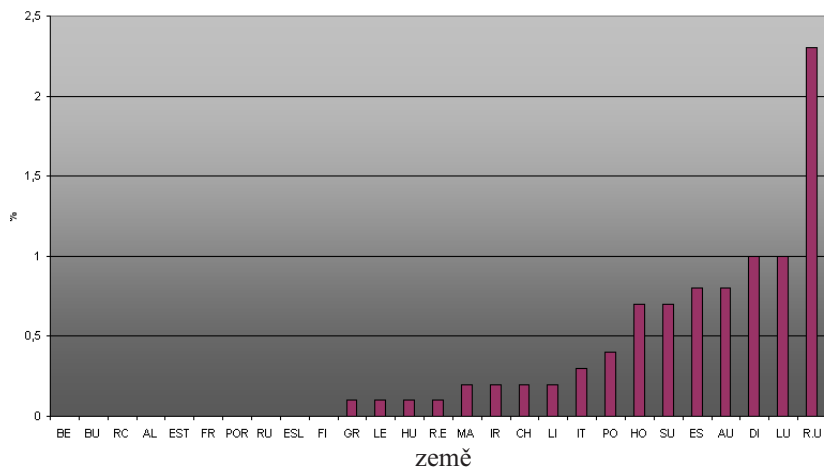
V důsledku růstu možností bezhotovostních plateb dochází k nárůstu mnoha druhů podvodů. V následujících odstavcích odkazujeme na zprávu Ontsi z roku 2008, která je publikována na webových stránkách Eurostat, a dokládá čísla stávající situaci. Je nutné zdůraznit, že je velmi obtížné získat údaje o tomto druhu podvodů, jelikož je to často zpracovááno s největší důvěrností správními úřady a některé případy se nikdy nedostanou na veřejnost.

Uživatelé e-bankovnictví



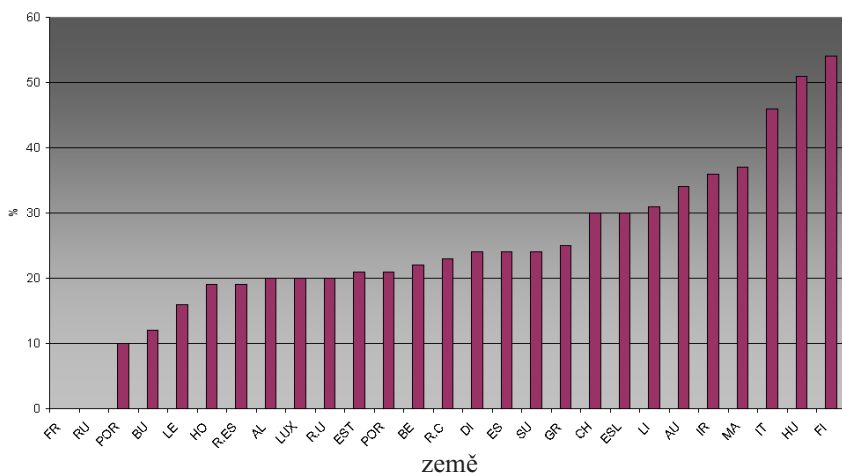


Internetové podvody při užití kreditních karet



Publikované údaje dokládají, že ve Velké Británii tento druh podvodů dosahuje 2,3 %, což je číslo, které přesahuje ostatní.

Bezpečnostní problémy způsobené informačními viry



Dále poukazujeme na skutečnost, že související problémy způsobené viry v zabezpečení dat, dosahují např. v Itálii, Maďarsku a Finsku zhruba 50%.

3. Různorodost podvodů při bezhotovostních platebních prostředcích



3.1. Karty

V současnosti je používání karet liž dobře zavedeno; průměrný počet karet na osobu je třikrát vyšší než počet karet v oběhu v roce 2000.

Co je elektronická karta?

Existuje široký sortiment karet. Nejčastěji používané karty jsou uvedeny dále.

1. DEBETNÍ KARTY

Debetní karta je plastová bankovní karta s magnetickým proužkem nebo nověji vybavená čipem, používaná k vyzvednutí hotovosti z bankomatu a rovněž k placení nákupů v obchodech, které mají terminály se čtečkami bankovních karet. Pro vyzvednutí hotovosti nebo pro nákup zboží je zapotřebí mít běžný účet s kladným zůstatkem u vydávající banky, jinak transakce bude zamítnuta.

2. KREDITNÍ KARTY

Kreditní karta, podobná debetní kartě, je plastová bankovní karta s magnetickou páskou nebo nověji vybavená čipem, používaná k vyzvednutí hotovosti z bankomatu a k placení nákupů v obchodech, které mají terminály se čtečkou bankovních karet. Rozdíl s debetní kartou je, že karta nabízí možnost pozdější platby za zboží.

Používáním kreditní karty má majitel karty přístup k úvěru, který byl předem dohodnut s bankou. Takto může majitel kartu použít k nákupu zboží a služeb nebo jednoduše vyzvednout hotovost do výše předem dohodnutého úvěrového limitu. Platba je prováděna na počátku následujícího měsíce nebo ve splátkách, které vedou k placení úroků.



3. ROZDÍL MEZI NÁRODNÍMI A MEZINÁRODNÍMI KREDITNÍMI KARTAMI:

MEZINÁRODNÍ KREDITNÍ KARTY se používají k nákupům v jakékoliv zemi na světě v jakékoliv měně.

NÁRODNÍ KREDITNÍ KARTY jsou omezeny na transakce ve měně a v zemi vydání.

4. KARTY OBCHODNÍCH DOMŮ

Tyto karty jsou vydávány obchodními domy, maloobchodními řetězci a komerčními sdruženími. Je to obvykle kreditní karta, jejímž účelem je zlepšit věrnost zákazníka, nabízející možnost shromažďovat body za nákup nebo využívat slevy.

5. POKLADNÍ KARTY

Tyto karty se objevily v nedávných letech, ačkoliv menší rychlostí než se očekávalo. Jejich funkce je nahradit hotovost při malých každodenních nákupech a sestává z karty (která může rovněž být jiným typem karty např. debetní kartou), která má zabudovaný mikročip. Čip zaznamenává množství peněz použitých pro další nákupy v podnicích s vhodným termínem. Karta může být dobита ve vydávající bance, v bankomatu, prostřednictvím webových stránek banky převodem prostředků z jiného účtu, prostřednictvím telefonního centra nebo převodem z jakékoliv banky.

3.2. Bankovní převody

Bankovní převody jsou způsobem převodu prostředků z účtu jedné banky na jiný účet, aniž by se fyzicky vyzvedávaly peníze. Může k němu docházet mezi účty patřícími jednotlivcům a společnostem ve stejné bance, mezi různými bankami v různých zemích nebo mezi účty různých majitelů účtů.



Druhy převodů

- V závislosti na místě převodu:
 - Národní převody: Převody mezi plátcem a příjemcem ve stejné zemi.
 - Mezinárodní převody: Převody mezi plátcem a příjemcem v různých zemích..
- V závislosti na spěšnosti:
 - Běžné: převody provedené v normálním časovém rámci.
 - Spěšné: převod provedený v kratším časovém rámci než je uvedeno.

Přímá platba

Toto je automatická platba z bankovního účtu založená na předchozí dohodě se společností (se kterou je uzavřena smlouva o službě) a bankou, která autorizuje platby. Tato metoda je velmi běžná při provádění pravidelných plateb např. účtů za veřejné služby. Přímé platby jsou obvykle zpoplatněny ročně nebo za šest měsíců, jak je předem určeno.

Poštovní poukázka

Toto je metoda platby, která spočívá na zaslání peněz od jednotlivce nebo společnosti prostřednictvím poštovní služby. Vydavatel platby pouze musí poskytnout identifikaci a umístění osoby nebo společnosti, která obdrží peníze.

Rysy:

- Peníze mohou být zasílány v dané zemi a do ciziny.
- Minimální množství je € 0.10.
- Dodání je provedeno na uvedenou adresu.
- Jsou přípustné osobní sdělení až do 140 znaků.

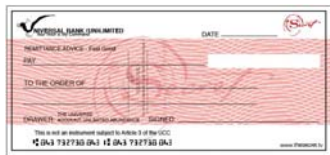


Druhy poštovních poukázek:

Existují dva druhy poštovních poukázek, které se hlavně liší datem dodání.

- Běžné: Doručení do tří až pěti dnů v národním měřítku, zatímco mezinárodní dodání závisí na poštovní službě druhé země.
- Okamžité: Doručení téměř okamžitě.

3.3. Šeky, směnky a dlužní úpisy



Šek je převoditelný cenný papír, kterým osoba, která je oprávněná vyzvedávat peníze z účtu zmocňuje jinou osobu k vyzvednutí určitého množství peněz, bez ohledu na přítomnost majitele bankovního účtu.

Druhy šeků

- Šek na doručitele: příjemce není specifikován.
- Šek na řad: příjemce platby je specifikován.
- Pokladní šek: vydávaný úvěrovou institucí pro platbu v jejích vlastních pobočkách a dceřiných společnostech.
- Potvrzený šek: když příjemce potřebuje být absolutně jistý, že existuje dostatek prostředků, které má platit banka .
- Křižovaný šek: šek na objednávku, který byl „křižován“ na přední straně vydavatelem, takže nemůže být vybrán hotově, ale pouze uložen na bankovní účet.
- Cestovní šeky: vydávané autorizovanými útvary pro platbu prostřednictvím poboček v zemi původu nebo v cizině.
- Šek, který má být uložen na účet příjemce: obsahuje podrobnosti o osobě nebo společnosti a účet příjemce. Tyto informace mohou být uvedeny na zadní straně šeku.



- Registrovaný šek: tento šek může být pouze vybrán osobou ve stejný den, ve kterém je požadován a ve stejné pobočce, kde byl vystaven

Směnka

Směnka je písemný příkaz od jedné osoby (vydavatele) druhé osobě (směnečníkovi) vyplatit určité množství peněz v budoucnosti (určené nebo určitelné) třetí straně (příjemci). Zapojení jednotlivci jsou:

- Vydavatel: osoba, která vydá platební příkaz a připraví dokument.
- Směnečník: osoba, která přijme platební příkaz a podepíše dokument, souhlasící s platbou, takto přijímá odpovědnost a uvede místo nebo adresu platby pro příjemce platby, který má platbu obdržet.
- Příjemce nebo adresát: osoba, která obdrží platbu v předepsané době.

Dlužní úpis

Dlužní úpis je dokument, který obsahuje bezpodmínečný slib osoby zaplatit určitou sumu peněz v předepsané době druhé osobě (příjemci) Hlavní rozdíl vůči šeku je, že jakmile je dlužní úpis vydán, je stanoveno, kdy platba může být provedena.

3.4. Platba mobilním telefonem/emailem: PayPal

Platba mobilním telefonem

Platba mobilním telefonem je služba, která umožňuje platby a další bankovní transakce provést v jakékoliv situaci, době nebo místě.

Systém se skládá z propojení jedné nebo několika elektronických karet vydávaných bankou s mobilním telefonem. To umo-



žňuje dobít vaši předplacenou kartu mobilního telefonu a zaplatit za internetové nákupy, taxíky a loterie a dávat dary atd. a rovněž kontrolovat bilance a pohyby na bankovním účtu, podobně jako u bankomatu.

Každá transakce umožňuje uživateli si zvolit jakoukoliv metodu platby, která byla aktivována na jeho účtu a akceptována organizací.

Existuje osobní identifikační číslo (PIN) vydávané bankou pro každou metodu platby, známé pouze majiteli účtu. Každá transakce je autorizována uživatelem uvedením PIN nebo kódu, který je dán vydavatelem pro každou metodu platby a je ekvivalentní ručnímu podpisu.

PayPal je systém

PayPal je systém platby online vyvinutý společností eBay Group. Je proto široce používán zákazníky tohoto druhu aukce a všeobecně pro transakce mezi jednotlivci.

Je to mezinárodní systém, který je k dispozici ve 44 zemích a 5 měnách (Eurech, US dolarech, librách, kanadských dolarech a japonských jenech). Platby jsou okamžité, bez ohledu na to, kde se nalézá nakupující.

Systém je založen na provádění plateb prostřednictvím emailu. Systém pracuje tím, že umožní uživatelům se registrovat pouze jednou s účtem jejich banky nebo podrobnostmi o kreditní kartě a pak zařídit anonymní platby z tohoto účtu nebo karty. Tyto platby jsou zařizovány jednoduše poskytnutím emailové adresy společnosti nebo jednotlivce, kterému chcete zaslat peníze. PayPal odpovídá za oznámení příjemci zasláním zprávy po internetu.

Služba je bezplatná pro klienta, zatímco prodávající je vystaven poplatku za příjem plateb. Provize jsou účtovány na počátku každého měsíce na základě objemu prodejů, které obchodník měl v předchozím měsíci.



4.1. Úvod

Každým rokem je zřejmý nárůst podvodů spáchaných organizovanými kriminálními gangy. Rozsah jejich aktivit je rozsáhlý: phishing, zlovolné kódy, kreditní karty, zasílání nevyžádaných emailů (spam), podvodných dopisů – scams atd. Tyto gangy pocházejí hlavně ze tří mezinárodních oblastí (východní Evropy, Brazílie a jihovýchodní Asie), nicméně následně používají zdroje z celého světa.

Používání zlovolných kódů a softwarových programů používaných pro krádež informací narůstá znepokojující rychlostí, do rozsahu, který zastiňuje nejpoužívanější metodu nedávné doby, phishing. Zlovolné kódy se používají ve vzrůstající míře pro ilegální získání informací a finanční zisk.

Používání zlovolných kódů vyžaduje vyšší stupeň obtížnosti při jejich navrhování, což naopak je činí obtížněji detekovatelnými.

Pokud se týká původu těchto zločinných praktik, Spojené státy vedou v seznamu případů phishing s 38 % z celkových počtů, jsou následované Tureckem (16,2%), Čínou (5,4%), Mexikem (4,7%), a Německem (3,9%) Spojené státy rovněž výrazně přesahují ostani jako nejčastější původce Trojského koně a přesměrování připojení (49,8%, respektive 51,8% z celkových počtů případů). V případě Trojského koně jsou následovány Ruskem (7,2%) a Austrálií (6,9%), zatímco ve zločinné praxi přesměrování připojení je nleduje na druhém místě Německo s 9,2% z celku.



Evropská komise uvádí, že více než 32 % uživatelů nezíská zpět své peníze, když se stanou oběťmi podvodů; takže spotřebitel je do určité míry bezmocný.



4.2 Phishing

Tento kriminální čin zahrnuje krádež hesel bankovních účtů majitelů účtů za účelem ukradení jejich peněz.

Jak se snaží podvést?

Podvodník známý jako "phisher" se vydává za důvěryhodnou osobu nebo podnik ve zdánlivě oficiální elektronické komunikaci obvykle emailem nebo podobně. To je prováděno na příklad jako hromadná zásilka uživatelům metod platby na základě zprávy, která se pokouší příjemce přesvědčit, že jsou kontaktováni svou bankou, která žádá o jejich přístupové kódy. Rovněž jsou uskutečňovány telefonické hovory.

Uživatel, jehož hesla byla podvodně vyžádána, může rovněž toto poznat prostřednictvím jiných metod např. nalezením založených potvrzení o platbě, tajným sledováním jeho pošty, vyhledáváním informací, které nebyly vymazány ze starého počítače atd.

Praktiky se týkají provádění nákupů online nebo telefonicky, jestliže všechny číslice a datum platnosti (které mohou rovněž být vypracovány zkusmo) jsou viditelné. Podvodníci jsou ochotni platit značné sumy peněz za získání seznamů platných čísel karet získaných tímto způsobem.



“osobní email”.

Tento druh podvodu se značně rozvinul. Původně byla použita sdělení, která se rozeslala nahodile na pokud možno co nejvíce adres v naději, že jeden z příjemců bude majitelem účtu v této bance. Dnes podvodníci propracovali své metody tak, že mohou dokonce detekovat, ke které bance uživatel patří, aby mu zaslali



4.3 Pharming

Pharming je sofistikovanější a nebezpečnější nová hrozba, která se skládá z falšování adres Domain Name Server (DNS) používaných uživateli. DNS servery odpovídají za směrování uživatelů na stránku, kterou chtějí vidět, ale během procesu, kdy uživatel píše adresu stránky, kterou chce vidět v prohlížeči, mohou být tyto údaje ve skutečnosti zaslány na jinou stránku vytvořenou hackerem, která vypadá stejná jako originál. Uživatel internetu pak důvěřivě zapíše důvěrné údaje, aniž si uvědomuje skutečnost, že informace je odesílána podvodníkovi.



Jak to funguje?

Tento podvod může být spáchán několika způsoby:

- Název domény může být vytvořen velmi podobným názvem k názvu webové stránky, aby se uživatel zmátl.
- Může být vytvořeno falešné propojení z jiných webových stránek, které vede na falešnou webovou stránku.
- Toto může být kombinováno s phishingem přidáním falešného propojení na email.

Zločinci se snaží získat osobní informace pro přístup k bankovním účtům, ukrást údaje totožnosti nebo spáchat jiný podvod jménem uživatele, což znamená, že cílem těchto útoků jsou banky a podobné finanční instituce.

Pharming je jasným případem měnící se doby, kterou poznáváme, pokud se týká internetových hrozeb. Ve vzrůstající míře útoky, ke kterým dochází nejsou zaměřeny pouze na ovlivnění mnoha uživatelů, ale na vytváření finančních zisků.



4.4 Spoofing

Tato metoda podvodu se zaměřuje na metodu krádeže identity obvykle spojenou se zlovolným nebo pátracím použitím.

Existují různé druhy v závislosti na technologii uváděné jako “IP spoofing” (možná nejvíce známé), “ARP spoofing”, “DNS spoofing”, Web spoofing a “email spoofing” ačkoliv všechny síťové technologie, které jsou náchylné ke krádeži identity mohou být všeobecně zahrnuty pod pojmenování “spoofing”.

Spoofing se používá pro mnoho různých účelů: primárně pro získání informací o uživateli, např. jaké navštěvuje stránky, hesla, soukromé informace o uživateli atd.

Útoky na zabezpečení na síti prostřednictvím spoofingu ohrožují soukromí uživatelů surfujících na internetu a rovněž integritu jejich dat.

4.5. Co jsou Trojské koně?

Trojské koně a červi (worms) jsou zlovolné programy, které jsou schopny zůstat v počítačích, aby umožnily přístup vnějším uživatelům prostřednictvím místní sítě nebo internetu s cílem shromažďovat informace nebo ovládat na dálku hostující stroj.

Trojský kůň sám není virus, ačkoliv teoreticky může být šířen a fungovat jako virus. Základní rozdíl mezi ním a virem je jeho účel. Aby program byl Trojským koněm, potřebuje pouze zpřístupnit a ovládat hostující počítač, aniž by si toho někdo všiml a obvykle se zdá být neškodný. Na rozdíl od viru, který je destruktivní, nemusí Trojský kůň nutně způsobovat poškození, jelikož to není jeho účel.

Trojský kůň je obvykle program umístěný v aplikaci např. v obrázku, hudebním souboru, nebo jiném nevině vypadajícím prvku, který se instaluje sám v operačním systému souboru, ve kterém je obsažen.



Co je jeho účelem?

Trojan se obvykle používá pro tajné získávání informací za použití metody pro instalaci softwaru, který umožní na dálku přístup ke sledování toho, co legitimní uživatel počítače dělá (v tomto případě Trojan je špionážním zbožím) a na příklad zaznamenává klávesnicové úhozy, aby získal hesla (když Trojan toto provádí nazývá se “registrační zařízení klávesnice”) nebo jiné relevantní informace pro spáchání podvodu.

4.6. Nigerijské dopisy

Řetězový mail se stal značně populární v nedávných letech (mail, který je zaslán každým příjemcem na jeho kontakty), který požaduje pomoc pro nemocného, opuštěná zvířata, nebo jakékoliv jiné způsoby zkonstruované pro apelování na smysly čtenáře. Avšak častěji tyto maily nejsou ničím jiným než jinou formou podvodu, podobnou těm, které byly dříve zmíněny.

Jak fungují?

Tyto dopisy mají formu emailu informujícího příjemce, že vyhrál v loterii nebo slosování nebo žádající o pomoc při vyhnutí se dani z kapitálového příjmu za značnou odměnu. Ve skutečnosti se pokouší podvést uživatele internetu, který je pak požádán o zaslání určitého množství peněz pro zaplacení celních poplatků, spotřebních daní, daní, odměny úředníkům atd., aby mohli obdržet odměnu, která se však nikdy neuskuteční.

Můžete získat zpět vyplacené sumy ?

Navzdory tomu, že to je technicky jednoduché, je toto jednou z neškodlivějších podvodných praktik pro oběti. Kromě toho je velmi obtížné získat zpět peníze, jelikož jsou obvykle zasílány prostřednictvím žir do zemí s malým, pokud vůbec, právním zabezpečením, kde peníze rychle zmizí ze zřetele.





4.7. Co je scam?

Toto je podvod, který kombinuje phishing s nigerijskými dopisy. Nejprve podvodník nabízí vysoce placené práce prostřednictvím chatů a blogů pravidelně navštěvovaných internetovými uživateli, a vyžádá si jejich jméno a bankovní účet, aby je mohl použít. Pak prostřednictvím phishingu, získá hesla od ostatních uživatelů a převody jsou uskutečněny prostřednictvím “prostředníka” (další oběti, která souhlasí s obdržení prostředků a pak je odešle, po odečtení provize, za účelem proprání peněz). Tato osoba si myslí, že uzavřela smlouvu na hospodaření s penězi a zašle peníze prostřednictvím žir do jiných zemí.

4.8. Libanonská smyčka

Je to podvod prováděný na bankomatech, zejména těch, které jsou instalovány na ulici, protože mají méně zabezpečovacích opatření.

Jak to funguje?

Modus operandi se často mění a my se zaměříme na tři nejběžnější:

Metoda 1

Podvodník vloží tak zvanou “smyčku” do drážky pro kartu, obvykle určitou délku magnetické videopásky, tak, aby bankomat nedetekoval kartu. Pak, když se objeví oběť a vloží kartu do bankomatu, ten se „ucpe“.

Pak kolem jde další člen podvodného týmu, předstírající, že je “dobrým Samaritánem” a nabízejícím pomoc. Nabízí svůj mobilní telefon a řekne oběti, aby kontaktovala banku a požádala o pomoc.

Na druhém konci linky je jiný podvodník, který požádá oběť o vytvoření 8 čísel do telefonu, kde poslední čtyři číslice jsou čísla PIN karty.



Jakmile toto bylo provedeno, oběť vidí že kartu bankomat nevrací a případně se vzdá a odejde, zanechávaje kartu v bankomatu, toto je okamžik, kdy první podvodník vyndá kartu a pak ji použije k vyzvednutí peněz zpětným vyhledáním čísla PIN ze svého mobilního telefonu.

Metoda 2

Je instalována videokamera, která zaznamená číslo PIN spolu s falešnou drážkou pro zachycení karty.

Poté co oběť vyzvedla peníze, kartu nelze vyndat.

Když oběť chce nalézt pomoc, podvodník získá zpět kartu, která může být nyní použita s číslem PIN zaznamenaným kamerou. Variace této metody je použití spolupachatele místo kamery, který se snaží získat PIN “nabídnutou pomocí”, zatímco oběť nedává pozor.

Metoda 3

Podvodník stojí vedle oběti.

Jakmile oběť vloží kartu do bankomatu podvodník upustí bankovku na zem a řekne oběti, že ji upustila.

Když oběť se ohne, aby zvedla bankovku, podvodník vymění kartu v bankomatu za jinou. Pak oběť se snaží vyzvednout peníze, ale nemůže, takže si vezme kartu a odejde.

Podvodník předstírá pomoc, aby zjistil PIN a může pak použít kartu k vyzvednutí peněz.



4.9 Skimming/carding

Je to způsob, který klonuje magnetickou pásku a může být proveden různými způsoby. Často se používá u podnikových zařízení, která používají nezabezpečené terminály prodejních míst (Point of Sale Terminals - PST) na příklad u benzinových stanic a restaurací. Je možné, aby číšník nebo obsluha pumpy byli členy gangu, takže když je provedena platba přes PST, může být použit ke klonování magnetické pásky.

4.10. Podvod zaměstnanců

Tento podvod není zvlášť běžný a je pouze zjištěn v izolovaných případech. Týká se ze zaměstnanců bank, na příklad patřících ke skupinám zločineckých hackerů, kteří mají přístup k číslům PIN klientů a ostatním kódům, které použijí ke spáchání podvodu..

4.11 Smishing

Je to variace phishingu, ve které jsou k získání informací použity zprávy SMS.

Jak to funguje?



Uživatel obdrží SMS, která ho vláká na telefonní čísla nebo provedení bankovních převodů za různými účely.

Odesílatel zprávy (ať je to automatický systém nebo jednotlivec) je obvykle odesílatel spamů, který se snaží převzít identitu známého, kolegy nebo společnosti ze seznamu kontaktů.

Oběť obdrží SMS říkající, že si předplatila on-line datovací službu (nebo jinou) a že tato služba bude připsána k účtu za telefon. Zpráva rovněž nabízí spojení k webovým stránkám z telefonu pro přerušení služby. Mnoho lidí je alarmováno obdržením této zprávy a provedou propojení, aby odvolali službu. Oběti jsou nyní tam, kde chce podvodník a mohou být vystaveni nedobrovolnému stahování Trojského koně nebo jiného druhu podvodného programu tím, že usilují o propojení..



Jinou praxí je zaslání zprávy, říkající, že banka provedla velkou platbu z účtu oběti, na kterou neexistují dostatečné prostředky. Při zavolání je oběť konfrontována sérií zaznamenaných zpráv, které je rafinovaně vedou k tomu, aby uvedla podrobnosti bankovního účtu.



4.12 Vishing

Způsob, který je podobný phishingu, ale s rozdílem, že místo zasílání emailů jsou uskutečňovány internetové telefonní rozhovory, které žádají čísla kreditních karet, PIN atd..

Jak to funguje?

Zločinec konfiguruje “válečné vytáčení” (tato metoda je založena na vytáčení série telefonních čísel, aby byla nalezena ta, která jsou připojena k modemu, aby umožnila připojení k jinému počítači) v určité oblasti.

1. Když je na volání reagováno, ozve se alarm a upozorňuje “spotřebitele”, že jeho karta je podvodně použita a že by měl okamžitě zavolat následující číslo. Číslo je falešné bezplatné telefonní číslo “banky”.
2. Když oběť zavolá na číslo, odpoví počítač, který sdělí klientovi, že jeho účet musí být ověřen a že musí uvést 16 číslic své kreditní karty.
3. Když oběť uvede číslo své kreditní karty “podvodník-vis-her” má všechny informace potřebné k provedení podvodných transakcí s kartou.



4. Hovor je často rovněž použit ke získání čísel PIN, dat platnosti, čísel účtů a jiných užitečných informací.

4.13. Podvody s šeky, směnkami a dlužními úpisy

Existuje mnoho druhů podvodů týkajících se šeků, směnek a dlužních úpisů, ale všechny začínají tím, že někdo dá oběti šek nebo žiro, které se zdají být pravé a požádá, aby hotovost na oplátku byla někam zaslána. Šek je falešný, ale může trvat týdny než to vyjde najevo. Pak banka oběti požádá o šek, který má být proplacen. Skutečnost, že oběť může dostat peníze na šek neznamená, že šek je skutečný a nakonec oběť odpovídá za šeky nebo žira, které ukládá nebo směňuje.

4.14. Podvod při bezhotovostních platbách

Jedná se o periodické připisování transakcí, které nebyly autorizovány, na vrub účtu. Je to možné na základě využití informací ze scamů (podvod zaměstnanců, phishing atd.). Jestliže není prováděna pravidelná kontrola bankovních účtů, pak majitelé bankovních účtů mohou se stát obětí tohoto druhu podvodu po dlouhou dobu. Jestliže je zjištěna platba za něco, co nebylo nakoupeno, musí být banka instruována, aby zrušila poplatek a odmítla budoucí platby.



5. Evropské předpisy týkající se podvodů u platebních metod a SEPA



Kompletní přezkoumání předpisů v tomto ohledu ještě něco členské země potřebují provést. Jestliže neexistují patřičné postupy, nebude snadné pro tento sektor překonat nedostatek důvěry, který nyní existuje mezi klienty bank. Je nutné upozornit na to, že ve skutečnosti existují bankovní předpisy pro elektronické bankovnínictví platné v měřítku celého společenství, ačkoliv jsou poněkud povrchní a potřebují důkladný a hluboký vývoj v každé zemi.

5.1. Současné předpisy

Zelená kniha Evropského společenství publikovaná v dubnu 2007 řeší retailingové finanční služby, běžné účty, platby, osobní půjčky a hypotéky, spoření, investiční a pojišťovací produkty nabízené jednotlivcům včetně malých investorů.

Citovaný dokument se snaží přimět členské státy, aby vytvořily a propagovaly jednotný trh retailingových finančních služeb a v podrobné analýze specifikuje jak finanční služby prováděné na dálku – telefon a internet – dosud reprezentují poměrně zdrženlivý přeshraniční obchod. To odráží dosud místní fragmentovaný trh, kde většina finančních činností probíhá v pobočkách a dceřiných společnostech.

V roce 2002 byla publikována Směrnice o finančních službách poskytovaných na dálku s cílem zvýšit důvěru spotřebitelů při používání přeshraničních služeb.

Tato směrnice se zabývá ochranou spotřebitele pokud se týká informací a rovněž jejich práv při zrušení smluv. Avšak toto dosud dává členským státům širokou možnost pohybu v relativně generalizovaných předpisech EU, ponechávaje vakuum s ohledem na začleněné fiskální aspekty při uzavírání smluv na přeshraniční finanční služby tak typické pro on-line bankovníctví.



Nástroj regulace	Aspekty, které reguluje	Další poznámky
Zelená kniha	Drobné finanční služby v jednotném trhu	
Zelená kniha 2007	Politika finančních služeb (2005-2010)	
Směrnice 2002/65/ES	Komeracionalizace finančních služeb poskytovaných na dálku	Mění směrnice 97/7/ES a 98/27/ES
Směrnice 2000/58/ES	Soukromí a elektronická komunikace	Změněná směrnici 2006/24/ES
Směrnice 2000/31/ES	SI a vnitřní elektronický obchod	Změněno s konečnou platností dokumentem COM 2006)334

(Pozn.: Česká relevantní legislativa – viz další výstupy zpracované v rámci projektu, zejména Studie)

5.2. SEPA: Jednotný prostor Euro plateb

Od zavedení Eura v roce 2002 byli spotřebitelé schopni provádět platby v jednotné měně po celé eurozóně. Když se toho dosáhlo, nadešel čas, kdy spotřebitelé mohou provádět platby, aniž by používali hotovost, z bankovního účtu kdekoliv v eurozóně za stejných základních podmínek, bez ohledu na to, odkud platba pochází.

SEPA se stane plnou skutečností, až všechny platby v Eurech prováděné v eurozóně budou považovány za vnitřní platby a současné rozlišení mezi národními a přeshraničními platbami zmizí. To vyžaduje nejen harmonizaci národních bankovních postupů, ale rovněž ve zvyklostech klientů v celé zóně.

Co je SEPA?

SEPA je zóna, ve které spotřebitelé, společnosti a ostatní ekonomické zainteresované strany mohou provádět a přijímat platby v Eurech uvnitř a vně národních hranic za stejných základních podmínek a se stejnými právy a povinnostmi, bez ohledu na tom, kde se v zóně nacházejí.

Cílem SEPA je přispívat k evropské integraci prostřednictvím konkurenceschopného a inovačního trhu malých plateb, což má



nabídnout lepší úroveň služeb, efektivnější produkty a levnější alternativy při provádění plateb.

Systém SEPA je založen na jednotné měně a jednotném souboru platebních nástrojů: převodů, přímých trvalých příkazů a plateb kartou, efektivní infrastruktura zpracování plateb, společných technických normách, společné obchodní praxi, harmonizovaném právním rámci a kontinuálním rozvoji nových zákaznických služeb.

Proč potřebujeme SEPA?

Ekonomie eurozóny běžně nevyužívá všechny výhody, které nabízí měnová unie. Klienti se setkávají s obtížemi při provádění malých přeshraničních plateb, jelikož tyto platby všeobecně vyžadují více času. Takto by Euro nemohlo být považováno za plně fungující jednotnou měnu. Bankovní sektor bude v rámci SEPA schopen nabídnout svým klientům nové nástroje plateb, založené na novém souboru pokynů, praxí a norem pro platby v Eurech.

Jaké jsou cíle SEPA?

- Vytvořit prostor, kde platby jsou prováděny soutěživě a inovačně, díky vysoké úrovni služeb, efektivním produktům a nízkým poplatkům.
- Platební nástroje regulované SEPA:
 - Bankovní převody od 28-1-2008
 - Přímé bezhotovostní platby
 - Platby kartou

Finanční instituce v SEPA odpovídají za kvalitu svých produktů a mohou nabízet svým klientům tyto zlepšené produkty, pokud jsou v souladu s definitivními rámci provozních předpisů a pokynů.



Bankovní převody v SEPA

Bankovní převody jsou prvním nástrojem, který prokazoval službu, což znamená, že nyní poslat převod ze Sevily do Helsinek je snadné, rychlé a spolehlivé jako posláni z Valencie do Bilbao.

Převody SEPA sdílejí následující charakteristiky

- Hodnota a měna: Eura bez omezení hodnoty
- Bod původu a místo určení: z účtu na účet, bez hotovosti
- Časový rámec: maximum 3 dny (D+3) z účtu na účet, ačkoliv to může být rychlejší
- Poplatky: Existuje vždy ustanovení o PODÍLU (náklady a poplatky vyplývající z transakce jsou sdíleny oběma stranami. Každá strana platí množství odpovídající jejich bance.) Spotřebitelské organizace jsou názoru, že sdílení nákladů musí být příznivé pro spotřebitele a že celkové náklady účtované v poplatcích by měly být rozděleny stejně mezi oběma stranami nebo podle jiné zavedené metody, ale nikdy by neměly překročit náklady předem uhrazené plátcem.

Výjimky v bankovních převodech SEPA (příklady):

- SEPA neplatí, jestliže kupující požaduje další službu: spěšné dodání, hodnotu stejného dne atd.



6.1. Jak se chránit proti platebním podvodům

Uživatelé musí provést řadu opatření. Dále jsou uvedeny některé praktické rady, které by měly být vzaty do úvahy, a rovněž znalosti týkající se vašich práv.

Rady o správném používání kreditních karet

- Vždy čtěte smlouvu
- Pořizujte si pouze karty, které potřebujete, nepodléhejte atraktivnímu designu nebo jiným aspektům.
- Nikdy nepřijímejte nevyžádané karty.
- Požadujte vyloučení podezřelých ustanovení, která banka může použít, aby se zbavila odpovědnosti.
- V případě pochybnosti vyhledejte nezávislou radu od spotřebitelského sdružení.

Praktické rady k ochraně vašich karet

- Nenoste u sebe svůj PIN. Naučte se ho a zničte ho nebo uchovávejte kopii na velmi bezpečném místě.
- Pro vaši vlastní bezpečnost vždy ukazujte svůj identifikační průkaz pouze při provádění nákupu na kartu.
- Nezanechávejte někde ležet příjmové doklady nebo jakékoliv papíry týkající se karty. Ty obsahují citlivé údaje. Ušchovejte je nebo zničte.
- Nikdy neztrácejte svou kartu z dohledu, vždy platte u pokladny.





Práva a rady pro uživatele převodů

Při provádění převodu nejlepší radou, která může být nabídnuta spotřebiteli, je znát svá práva předem a jestliže nejsou splněna požadovat jejich splnění.

Zde je uveden seznam vašich práv:

- Spotřebitel má právo znát potřebné informace před tím než provede platbu. Banka musí zajistit, aby její klienti si byli vědomi plných nákladů na operaci a věnovat zvláštní pozornost skutečnosti, že když klient chce převádět prostředky ze svého účtu, je si plně vědom všech alternativních metod a nákladů souvisejících s každou metodou.
- V případě, že převod není proveden, klientovi musí být poskytnuta plná náhrada. Náhrada musí zahrnovat náklady na převod plus jakékoliv vzniklé náklady a právně uplatněný úrok. Banka je povinna podle zákona provést náhradu do 14 pracovních dnů od data žádosti.

Rady pro vyzvedávání peněz v bankomatech

- Nejprve zkontrolujte zda všechno je tak, jak má být, jelikož bankomaty jsou někdy narušeny, aby umožnily získat PIN nebo hotovost.
- Zkontrolujte zda existuje pouze jedna štrbina pro kartu a že nadměrně nevyčnívá z bankomatu. Zkontrolujte zda existuje pouze jedna klávesnice a že se zdá být normální. Je vhodné učinit jiná opatření jako zavřít za sebou dveře a přesvědčit se, že vás nikdo dovnitř nenásledoval.
- Jestliže vás někdo požádá o pomoc, řekněte mu, aby použil intercom a nikdy mu nedejte svůj PIN.

Zabezpečení internetu

Zde uvádíme některé podstatné rady, kterými byste se měli řídit pokud se připojujete k síti:



- Pravidelně aktualizujte software.
- Periodicky zkontrolujte zabezpečení vašeho připojení (podvodné porty, antivirové programy, bezpečnostní zábrany - firewalls, citlivé informace o účtech atd.).
- Provádějte pravidelné zálohování dat.
- Vypněte počítač, když ho nepoužíváte.
- Dejte pozor při stahování softwaru, stahujte pouze z bezpečných zdrojů.
- Konfigurujte vaše navigační zařízení a programy s nejvyšší úrovní zabezpečení.
- Nevěřte přímým propojením na stránky, jelikož tato propojení vás neuvědomí vždy na požadovanou stránku.
- Citlivé údaje - například čísla účtů - vkládejte pouze tehdy, když stránka je zabezpečena: za bezpečné jsou považovány např. stránky začínající s „http“.
- Konfigurujte adresu osobního emailu, abyste zasílali a obdrželi zprávy v textovém módu: html nenabízí mnoho výhod v textu a je problematictější z hlediska zabezpečení.
- Zakódujte* vaše nejdůležitější zprávy a soubory tak, aby při jejich čtení třetími stranami jim bylo těžko rozumět.



**Zakódovat znamená transformování údajů do tajného kódu, který může být pouze dešifrován zamýšleným příjemcem. Za určitou dobu a zdrojů IT mohou být všechny zakódované zprávy dekodovány, ale to vyžaduje enormní dobu a IT zdroje. Jednoduše řečeno, zakódování je způsob skrytí vašich souborů a emailů před hackery. vaše soubory jsou převedeny do kódu (což zřejmě nemá smysl u nahodile vybraných dopisů a položek). Abyste zakódovali soubor, zablokujte ho úhodem na klávesnici, který reprezentuje frázi hesla. Abyste zakódovali zprávu, zablokujte ji řadou úhozů na klávesnici za použití fráze hesla. Tato zpráva může být pouze otevřena zamýšleným příjemcem za použití jeho vlastní fráze hesla.*

Rady a opatření týkající se elektronického nakupování a online bankovníctví

Velká pozornost musí být věnována tomu, aby server byl bezpečný. Abyste zjistili, zda je bezpečný, musí splňovat následující požadavky:

- Dole na prohlížeči se objeví ikona uzavřeného visacího zámku.
- Adresa stránky začíná s https místo běžnějšího http. Vždy pracujte se zabezpečenými stránkami, nikdy nezasílejte bankovní podrobnosti prostřednictvím nezabezpečených stránek nebo emailů.
- Vždy si uschovejte vytištěnou a elektronickou kopii účtů za nákupy online.
- Vždy zkontrolujte platnost certifikátů (tím, že kliknete na ikonu uzavřeného visacího zámku), že jsou v souladu s požadovanou bankou a že jsou běžné a platné.
- Vezměte do úvahy, že banka Vás NIKDY nepožádá o sdělení důvěrných informací emailem nebo telefonem.
- Vyhněte se používání veřejných zařízení (internetových kavárnen, nádraží, letišť atd.), abyste zde prováděli on-line obchodní transakce.



- Deaktivujte volbu “automatického vyplňování” jestliže získáváte přístup prostřednictvím zařízení, které není vaším obvyklým zařízením nebo které sdílíte s jinými lidmi.
- Uzavřete relaci, když skončíte, abyste zabránili jiným lidem k přístupu k vašim posledním pohybům, ke změně vašich kódů, k provádění převodů atd.
- Instalujte nástroj proti podvodům, abyste zabránili přístupu na podvodné stránky.



6.2.Co dělat, když jste byli vystaveni podvodnému jednání

Toto jsou první kroky, které byste měli učinit, jestliže objevíte, že jste se stali obětí podvodu:

- V případě ztráty nebo krádeže karty, okamžitě to oznamte bance nebo vydavateli tak, aby karta byla zrušena (osobně na nejbližší pobočce nebo telefonicky).
- Oznamte krádež policii: jestliže máte jakoukoliv dokumentaci týkající se podvodu, uveďte ji. Jestliže nemáte žádnou dokumentaci, postačí zpráva.
- Kontaktujte vaši banku, předložte identifikační průkaz a policejní protokol.
- Jestliže je do transakce zapojena i jiná banka (se kterou nemáte přímý vztah, ale které pravděpodobně něco dlužíte, nebo obchodu, kde jste provedli nákup) kontaktujte je,



abyste je informovali o situaci. Předložte kopii policejního protokolu.

- Snažte se zjistit, zda nevznikly vaším jménem nějaké dluhy, nejlépe prostřednictvím vaší banky nahlédnutím do registru dlužníků a neplatičů.





- Consumers in Europe: Facts and Figures on services of general interest. 2007 Edition. Eurostat, European Commission.
- Informe anual Ontsi 2008.
- European Financial Integration Report, 2008.
- World Payments Report 2008.
- Consejos generales de seguridad, Inteco 2007.
- Fraude en Internet, Inteco.
- Impositores y Usuarios, n°74 (Verano 2007). Dossier "El Euro de los medios de pago", pp. 19-23
- Global Phishing Survey: Domain Name Use and Trends in 2007. Mayo 2008. APWG (Anti Phishing World Group)



Kontakty

- Eurostat
<http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/home/>
- Evropská komise
http://ec.europa.eu/index_cs.htm
- Evropský parlament
<http://www.europarl.cs>
- Česká národní banka – ochrana spotřebitele
http://www.cnb.cz/cs/dohled_fin_trh/spotrebitel/index.html
- Ministerstvo průmyslu a obchodu – ochrana spotřebitele
<http://www.mpo.cz/cz/ochrana-spotrebitel/>
- Česká obchodní inspekce – Evropské spotřebitelské centrum
<http://www.coi.cz/cs/esc-2.html>
- Finanční arbitr
www.finarbitr.cz
- Sdružení českých spotřebitelů
www.konzument.cz

Praha, ústředí SČSIng. Libor Dupal, Ing. Libor
Novák

Budějovická 73, 14000 Praha 4

261263574;
spotřebitel@regio.cz**Jihočeský kraj a PLZEŇSKÝ KRAJ**

Marie Beránková

Pražská 33,
384 22 Vlachovo Březí388 329 190,
marie.ber@tiscali.cz**Karlovarský kraj**

ESPRO, s.r.o.

Svobody 36,
350 02 Cheb354 433 413
espro@cbox.cz**Ústecký kraj**YMCA v Ústí nad Labem
Filip HušekHradiště 4,
400 01 Ústí nad Labem
(budova kláštera sv.
Vojtěcha)475 220 831
usti@ymca.cz**Liberecký kraj**

Petr Jirásko

Družstvo EKON,
Valdštejnská ul. 381/6
460 01 Liberec 1777 700 068
petr@jirasko.cz**Jihomoravský kraj**Sdružení českých spotřebitelů
Ing. Miloš KolářNám. Svobody 18/210
669 02 Znojmo515 224 923
jimorava@regio.cz**Moravskoslezský kraj**

Jana Weberová

ELIM CENTRUM
Rolnická 21A,
747 05 Opava - Kateřinky553 653 239
elimopava@elimopava.cz**Královéhradecký kraj**RKM Hradec Králové
Petr KrejcarTř. Karla IV. 430, 500 02
Hradec Králové,tel. 495215266,
fax. 495220615
krejcar@regio.cz**ADICAE**Asociación de Usuarios
de Bancos, Cajas de Ahorros y Seguros.

odporováno Programem Evropské komise - GR pro spravedlnost, svobodu a bezpečnost: Prevence, připravenost a řízení následků terorizmu a jiných bezpečnostních rizik