

**FA**KANCELÁŘ FINANČNÍHO ARBITRA
ORGANIZAČNÍ SLOŽKA STÁTU

Zpravodaj finančního arbitra 01/2012

*Vážení čtenáři,*

dovolte mi, abych vám představila první vydání obnoveného občasníku vydávaného finančním arbitrem – Zpravodaje finančního arbitra.

Cílem Zpravodaje finančního arbitra je informovat veřejnost o činnosti finančního arbitra, ale také přispívat k lepší informovanosti a finanční vzdělanosti veřejnosti. To vše ve formě, která jak věřím bude poutavá, zábavná a přitom poučná.

Zpravodaj finančního arbitra se skládá ze tří hlavních částí, které budou tvořit, v různých obsahových obměnách, trvalou strukturu každého jeho vydání. V první části vás budeme prostřednictvím úvodního slova stručně informovat o tom, co je v námi sledované oblasti finančních služeb nového a co vás v aktuálním čísle zpravodaje čeká. Posláním druhé části Zpravodaje finančního arbitra je prostřednictvím skutečných příběhů čtenáře upozorňovat na úskalí, kterým mohou při využívání finančních produktů (bankovních účtů, platebních karet, spotřebitelských úvěrů atd.) čelit. Třetí část má za úkol seznámit veřejnost s odbornými tématy, která jsou zajímavá a přitom mohou čtenářům pomoci pochopit jednotlivé aspekty fungování finančního trhu, jednotlivých finančních produktů a služeb. Tato témata volíme tak, aby pomohla objasnit často kladené otázky, s nimiž se na arbitra obracíte, a aby přispěla k odstranění pochybností či nejasností v praktických záležitostech, s kterými se při využívání finančních služeb často setkáváte.

Zároveň bych byla ráda, abyste tento občasník vnímali jako otevřené médium, na jehož obsahu se sami můžete podílet. Proto nás kdykoliv kontaktujte, pokud budete mít k některému tématu otázku, budete se chtít podělit o své zkušenosti, nebo byste rádi, abychom se konkrétnímu tématu věnovali v některém z dalších čísel zpravodaje. Rádi se vašimi podněty necháme inspirovat.

Přeji vám inspirativní čtení!

Mgr. Monika Nedelková, finanční arbitr

KANCELÁŘ FINANČNÍHO ARBITRA
ORGANIZAČNÍ SLOŽKA STÁTULegerova 1581/69, 110 00 Praha 1 – Nové Město
IČ 72546522
tel. 257 042 094, e-mail: arbitr@finarbitr.cz
www.financniarbitr.cz

**FA**KANCELÁŘ FINANČNÍHO ARBITRA
ORGANIZAČNÍ SLOŽKA STÁTU

Zpravodaj finančního arbitra 01/2012

Finanční arbitr jako zákonem zřízený mimosoudní orgán pro rozhodování některých sporů na finančním trhu přináší nejširší veřejnosti svůj nový zpravodaj a v něm příběhy a případy, které se staly a které finanční arbitr řešil.

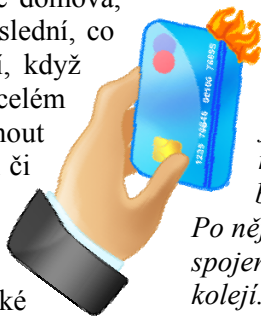
Zneužití platební karty v kruhu rodinném aneb důvěřuj, ale prověřuj; případ nezdárného syna

Mnozí jsme zažili tuto situaci – jsme v teple domova, odpočíváme po náročném dni v práci, a to poslední, co se nám chce, je vyjít ven do blátivého počasí, když pouhá představa tohoto zážitku nás zamrazí po celém těle... a právě tehdy se objeví potřeba poskytnout někomu blízkému, ať je to dcera, vnuk, manžel či přítel, hotovost, kterou u sebe momentálně nemáme. I když víme, že myšlenka, která nás zrovna napadá, není rozumná, podléháme naší lenosti a opouštíme naše pravidla a zvyky: blízké osobě, se snahou jí vyhovět a zároveň se vyhnout „nucené“ procházce, vložíme platební kartu do ruky se slovy: „Tak si do toho bankomatu zajdi. Tady máš PIN – je to 1928. A vezmi si účtenku.“ Právě jsme se vyhnuli nepříjemnému zážitku, blízkému člověku přece můžeme věřit. Většinou to bývá pravda – nic se nestane, dojde k výběru a blízký odpovědně vrátí kartu a na PIN zapomene. Jenže vězte, že i při tomto pozitivním scénáři vývoje událostí již došlo k něčemu špatnému. Porušili jsme několik zákonných i smluvních povinností.

Paní Jitka pracovala jako kuchařka v jídelně gymnázia. Nejen z důvodu zaslání platu si zřídila bankovní účet u banky, ke kterému obdržela platební kartu. Na účet si nechala zasílat svoji výplatu i z druhé práce a výživné na svoji nezletilou dceru, tedy její veškeré příjmy. Z účtu platila nejrůznější závazky a často při jejich placení používala platební kartu. Platební kartou platila v obchodech, restauracích a vybírala minimálně třikrát do měsíce hotovost.

Jednoho letního dne se Jitka vrátila s rodinou z dovolené a již při otevření branky vedoucí k domu se ji zmocnilo neblahé tušení. Jakmile se dostala ke dveřím, její tušení se pomalu, ale jistě naplňovalo – dveře byly

vypáčeny a bylo jisté, že byli vykradeni. Jeden z prvních nepříjemných úkolů, které musela Jitka vyřešit, bylo zablokování platební karty, kterou zloději také ukradli. Proto okamžitě informovala banku o krádeži platební karty a ta ji ihned zablokovala. Díky bleskurychlé reakci Jitky zloději nestihli napáchat další škody. I když paní Jitka nebyla tak hloupá, aby nechávala u platební karty PIN a nosila jej prozíravě v hlavě, bylo možné, že ke zneužití karty mohlo dojít. Zloději jsou vynalézaví a neznalost PIN je bohužel často nezastaví.



Paní Jitka obdržela novou platební kartu a k ní stejný PIN jako ke staré. Jitka si jej nezměnila, jelikož se domnívala, že starou kartu již nikdo nemůže použít. Tato domněnka byla správná – bankou znehodnocenou kartu již nelze použít. Po nějaké době, po úklidu a všech těch nepříjemnostech spojených s vyloupením, se Jitčin život vrátil do starých kolejí. Po čase si uvědomila, že na její adresu přestaly chodit výpisy z účtu. To ještě nevěděla, že nejde o náhodu, ale proradný čin někoho v jejím okolí. Jaké překvapení následovalo, kdy po čtyřech měsících při náhodné kontrole účtu zjistila, že je na něm o osmdesát tisíc méně, než by mělo být!

To, že Jitka nekontrolovala stav účtu častěji, byla bezezporu její chyba. První myšlenka, která ji však napadla po výčitkách, kterými se častovala, byla, že zloději zneužili její starou kartu. To však nebylo možné, řekla banka i finanční arbitr, na kterého se Jitka obrátila o pomoc. Následně při kontrole dodatečných výpisů z účtu začala objevovat zlou pravdu – týden co týden jí mizelo z účtu několik tisíc – v době, kdy vypomáhala v místní restauraci a peněženku nechávala v domě.

Doma byl jen její syn...

Banky a platební instituce, které vydávají platební karty, vás při zřízení platebního účtu seznamují s pravidly poskytované služby, vašimi právy i povinnostmi, a to písemně v podobě smluvních podmínek a pravidel stanovených pro používání platební karty. Tím, že tyto dokumenty podepíšete, se zavazujete k tomu se jimi řídit. Mezi základní pravidla nakládání s platební kartou patří, abyste ji nikomu nikdy nepůjčovali a už vůbec neprozrazovali

Legerova 1581/69, 110 00 Praha 1 – Nové Město
IČ 72546522

tel. 257 042 094, e-mail: arbitr@finarbitr.cz
www.financniarbitr.cz

KANCELÁŘ FINANČNÍHO ARBITRA
ORGANIZAČNÍ SLOŽKA STÁTU

**FA**KANCELÁŘ FINANČNÍHO ARBITRA
ORGANIZAČNÍ SLOŽKA STÁTU

Zpravodaj finančního arbitra 01/2012

PIN. PIN je osobní identifikační bezpečnostní číslo, které banka nebo platební instituce sdělí při vydání platební karty pouze jejímu držiteli. Za pomoci PIN pak autorizujete jakýkoliv požadavek na výběr z bankomatu či při platbě v obchodě. Tím, že někomu svoji platební kartu půjčíte a prozradíte svůj PIN, si koledujete o velký průšvih - banky a platební instituce totiž na takové použití platební karty spolu s PIN cizí osobou hledí, jako kdybyste ji použili vy osobně, protože platební karta je vaším platebním prostředkem (platební karta nemá co dělat v cizích rukou) a PIN je klíčem k jejímu použití – autorizujete jím váš požadavek na výběr z bankomatu či platbu v obchodě. Pro případ zneužití nebo dokonce ztráty či krádeže je vždy nutné takovou ztrátu okamžitě oznámit bance či platební instituci. Tak platební kartu zablokujete a již nikdo vám peníze z bankovního účtu ukradenou kartou nevezme!

Problémem při svěření platební karty a PIN blízké osobě bývá, že v případě, že tato osoba vaší důvěry zneužije a peníze z účtu bez vašeho souhlasu vybere, nemáte šanci na vrácení ukradených peněz bankou nebo platební institucí. Přitom často nemusíte mít o tom, že vaši platební kartu někdo zneužívá, dlouhou dobu vůbec ponětí. Podezřelé výběry můžete při další neopatrnosti zaznamenat z výpisů i po měsíci – pokud je váš blízký podvodník důkladný a vy velice neopatrní, i po měsících několika. Vzhledem k tomu, že si myslíte, že platební kartu máte fyzicky pořád u sebe, netušíte žádné nebezpečí, natož abyste bance či platební instituci ohlásili její ztrátu či krádež. Výsledkem může být kruté vystřízlivění z projevené důvěry a ztráta třeba i několika desítek tisíc...

Platební karta v autě není v bezpečí! PIN si pamatujeme

Podobné platí i v dalším případě. PIN nesděluje osobám blízkým v žádném případě – nejen proto, aby nebyly

vystaveny pokušení kartu zneužít jako v předchozím případě, ale proto, že vám to banky zakazují a pokud vznikne škoda a sdělení PIN je prokázáno, jde o hrubou nedbalost z vaší strany se závažným následkem – odpovídáte v plném rozsahu za vzniklou škodu.

Taková odpovědnost nastala i v případě pana Jirky z Karlovarského kraje. S manželkou potřebovali nakoupit vybavení do domácnosti, proto se vydali do nákupního centra. V autě však nechali téměř vše, včetně platební karty pana Jirky s PIN označeným v mobilu manželky. Jedinou věc, kterou si vzali s sebou, byla peněženka manželky. Tím, že Jirka prozradil manželce PIN, která si jej poznamenala do mobilu, navíc jej označila jako PIN, došlo k dvěma zásadním pochybením. Jirka porušil povinnost nikomu neprozrazovat PIN a uložením PIN do mobilu, byť manželky, se značně zvýšilo riziko jeho prozrazení a následného zneužití platební karty. K tomu také následně došlo. Během nákupu auto navštívili zloději a kompletně ho vykradli. Zmizela mimo jiné Jirkova karta a manželčin mobil s uloženým PIN.

Co následovalo dále? Zloději znali situace a chyb občanů věděli přesně co dělat. Netrvalo dlouho a PIN byl v manželčině mobilu objeven. Během deseti minut vybrali z účtu pana Jirky 24.000,- Kč! Jirka, i přesto, že se zachoval správně a okamžitě kartu na lince banky zablokoval, o peníze přišel. Bylo totiž zjištěno, že výběry proběhly před blokací karty – zloději jsou opravdu rychlí – tedy výběr byl z pohledu banky autorizován, byl proveden platnou platební kartou po správném zadání PINu. Muselo se tedy posuzovat, zda-li ze strany pana Jirky nenastala nedbalost, která umožnila výběry peněz. Bylo shledáno, že pan Jirka byl hrubě nedbalý, protože prozradil PIN cizí osobě, není jakkoliv důležité, že šlo o manželku, a k tomu neochránil PIN – nechal ho zapsaný v mobilu, který byl v bezprostřední blízkosti platební karty! Jirka tak už jen může doufat, že se podaří odhalit pachatele dříve, než peníze utratí.

Jak ochránit platební kartu:

- nikdy nesděluje PIN jiné osobě
- PIN neuchovávejte spolu s kartou
- při zjištění ztráty/krádeže karty ihned kontaktujte banku

FAKANCELÁŘ FINANČNÍHO ARBITRA
ORGANIZAČNÍ SLOŽKA STÁTULegerova 1581/69, 110 00 Praha 1 – Nové Město
IČ 72546522
tel. 257 042 094, e-mail: arbit@finarbitr.cz
www.financniarbitr.cz

Bezhotovostní podvody v ČR

V dnešním čísle zpravodaje vám přinášíme přehled podvodných praktik zaměřených na zneužití platebních karet a systémů elektronického bankovníctví. Vlivem technologického vývoje i znalostí podvodníků dochází k rychlému vývoji především v oblasti techniky získávání citlivých údajů a jejich následného zneužívání. Při zneužívání je možné hovořit o útocích na platební prostředek, např. platební kartu (skimming) a o útocích na lidskou důvěřivost (phishing).

Libanonská smyčka

V současné době je to již ojedinělý způsob, který způsobí, že platební karta se nedostane do bankomatu, ale ani zpět. Toto je zabezpečeno speciálním dodatečným zařízením instalovaným podvodníkem na bankomat. Podvodník je v blízkém okolí a postiženému nabídne „pomoc“ s podmínkou zadání PIN. „Pomoc“ se nezdaří, klient odchází bez karty, kterou podvodník následně vytáhne zpět a zneužije ji dříve, než dojde k její blokaci. Proti tomuto způsobu dnes většinou existuje účinná obrana v podobě dodatečných ochranných adaptérů instalovaných na bankomat.

Skrytá kamera

Pomocí malé skryté kamery podvodník zjišťuje PIN. Často je využívána v kombinaci s libanonskou smyčkou nebo skimmingem, někdy při platbě u obchodníka. Obrana spočívá ve skrytém zadávání PIN, např. zakrytím klávesnice bankomatu rukou. Důležité je si uvědomit, že skrytou kamerou může být i záznamové zařízení na mobilních telefonech, kdy může při nepozorném použití platební karty dojít k nahrání jak čísla karty, doby platnosti, CVC/CVV kódu, podpisu, a to např. při platbě „ve frontě“ u obchodníka, kdy osoba stojící poblíž může prostřednictvím mobilního telefonu toto velice jednoduše zaznamenat.

Dotekové senzory

Tento poměrně vzácný způsob získání PINu spočívá v instalaci senzorů na klávesnici bankomatu nebo např. na vstupní dveře do samoobslužné zóny

s bankomatem. Díky senzorům pachatel zjistí, která tlačítka a v jakém pořadí byla při zadání PINu zmáčknuta. Tento postup může být kombinován s účelovou krádeží karty, přepadením nebo jiným způsobem získání platební karty postiženého. Nejlepší obranou je obezřetnost při nakládání s platební kartou.

Padělky karet

Na padělcích se nejvíce podílejí kriminální skupiny z různých oblastí celého světa. Po zjištění citlivých dat dochází k promptní výrobě padělku, který je poté protizákonně zneužíván. Zařízení pro výrobu padělků může být o velikosti osobního kufříku a rychlost výroby takovéto karty je otázkou několika minut od zjištění citlivých údajů. Proti padělkům se brání samotné karetní společnosti i banky zaváděním nejrůznějších ochranných prvků a technického zabezpečení.



Zneužití pomocí internetu

Prostřednictvím internetu může dojít k přímému zneužití platební karty nebo bankovního účtu, ale také k nepřímému zneužití databáze obchodníka, který má evidenci karet svých zákazníků. V České republice je toto riziko prakticky

vyloučeno vzhledem k provozování internetových plateb pomocí 3D Security. Toto riziko může být zvláště u amerických a asijských obchodníků, v Evropě je minimální. Obranou je využívání jen zabezpečených forem plateb, vhodné jsou kreditní nebo virtuální karty.

Skimming

Jedná se o postup, při kterém jsou originální údaje z magnetického proužku karty elektronicky zkopírovány na jinou kartu, samozřejmě bez vědomí právoplatného držitele karty. Při kopírování dochází k záznamu PIN a dalších údajů o držiteli karty. Nedochází ke kopírování všech ochranných prvků (jako např. kódů CVC2/CVV2) a zneužití vyrobeného padělku platební karty bez těchto ochranných prvků, např. pro výběr z bankomatu, kde je kontrolována tzv. druhá stopa, pak není možné. Ve světě ale existují banky, které ochranné prvky svých

karet nekontrolují a na těchto bankomatech pak je možné padělek použít k úspěšnému výběru.

Phishing

Tato podvodná technika útočí na lidskou důvěřivost; dochází při ní k zneužití emailové pošty s cílem získání identifikačních údajů; riziko spočívá v tom, že zpravidla do e-mailového formuláře vyplní poškozený číslo své platební karty s dalšími osobními údaji; e-mail, který se jeví, že byl odeslán vaší bankou, však je podvodný, a pokud dojde k zadání k těmto citlivým dat, může dojít v krátkém časovém sledu k výrobě padělků platební karty a k jejímu zneužití – během několika minut může dojít k výběrům z bankomatu v zahraničí.

Pharming

Tato podvodná praktika má v zásadě dvě podoby. První podoba pharmingu je sice efektivní, ale pro podvodníka, který chce jejím prostřednictvím získat citlivé údaje značně obtížná. Spočívá v tom, že je napadán Domain Name System (dále jen DNS). DNS je systém doménových jmen, která jsou hierarchicky uspořádána. Hlavním úkolem systému a příčinou jeho vzniku jsou vzájemné převody doménových jmen a IP adres, což jsou čísla, která jednoznačně identifikují síťové rozhraní v počítačové síti - internetu. Zjednodušeně řečeno, identifikují konkrétní počítač. Celý systém je realizován protokolem stejného jména, jehož prostřednictvím jsou vyměňovány citlivé informace, tedy i ty, které prostřednictvím pharmingu získají podvodníci. Klient zadá ve svém internetovém prohlížeči nějakou adresu. Při jejím zadání ale nedojde k jejímu překladu na správnou IP adresu, ale na adresu, kterou zadali podvodníci. Pokud by se pak podvodníkům podařilo změnit DNS záznam klientovy banky, bude spojení s bankou pak přesměrováno na jiný kanál, jehož www stránky, připravené podvodníky, budou velice podobné oficiálním stránkám klientovy banky. Při následném přihlášení klienta ke komunikaci s bankou získají podvodníci citlivé údaje a bude následovat odčerpání finančních prostředků z kli-

entova účtu. Tato metoda je pro zákazníka obtížně odhalitelná, avšak na straně podvodníka vyžaduje již velmi pokročilé technické znalosti a odpovídající vybavení.

Druhá podoba pharmingu je pro podvodníka jednodušší, a proto je i více používána. Lze se jí ale snáze ubránit. Spočívá v tom, že podvodníci napadají nikoliv IP adresy na DNS serverech, ale útočí na jednotlivé počítače. Velice zkráceně - podvodník se snaží o zapsání adresy jeho www stránky s doménou bankovníctví do tzv. host souboru, který pracuje v určeném operačním systému, podobně jako DNS. Obsahuje tedy IP adresy a korespondující domény. Pokud se mu to podaří, je při přihlašování klienta do internetového bankovníctví zobrazena podvodná stránka a útočník získá citlivé údaje pro manipulaci s finančními prostředky na účtu klienta. Pharming se do klientova počítače může dostat jako trojský kůň, který je poslán v příloze nějakého e-mailu, může být stažen apod.

A jaká je obrana proti pharmingu? Způsobů jak se bránit je více a můžeme je rozdělit do dvou skupin. První skupina spočívá v softwaru. Znamená to např. používat vysoce kvalitní antivirový program, provádět jeho pravidelnou aktualizaci, používat silný firewall atd. Druhá skupina spočívá v obezřetnosti samotného uživatele (klienta), který s počítačem pracuje. Obezřetnost znamená nestahovat z internetu neznámé aplikace, neotevírat odkazy v e-mailech z neznámých adres, neinstalovat programy neznámého původu, neotevírat podezřelé přílohy e-mailů zaslaných z adres vašich známých, dokud si neověříte, že e-mail skutečně odeslali sami apod.

Spoofing

Je technika, která není v České republice dosud rozšířena. Spoofing znamená doslova napálit, převést, vést za nos; patří mezi nejnebezpečnější zbraně těch, kteří chtějí neoprávněně proniknout do cizích sítí. Podstata podvodu spočívá v tom, že se určitý uzel sítě vydává za „někoho jiného“. V důsledku tzv. „osahávání“ serverů nebo lokál-



ních sítí mohou být za určitých podmínek zjištěna citlivá data, která mohou být následně zneužita. Tato technika je vysoce sofistikovanou verzí internetového pirátství, proti kterému se banky (vůči nimž je zejména namířena) brání vývojem robustních IT systémů na ochranu klientských dat.

Trashing

Je to další z „moderních“ způsobů podvodů; je rovněž založený na zjištění citlivých dat. Název je odvozen od anglického trash (koš). Jde v podstatě o „vybírání odpadků“, z nichž lze zjistit řadu „zajímavých“ informací. Výjimkou nejsou přístupová hesla, zdrojové kódy apod. Proto je nutné pečlivě dbát na řádnou skartaci dokumentů a bezpečnou likvidaci elektronických dat.

Tato metoda je opět zaměřena spíše na banky a velké společnosti, než na jednotlivé uživatele. I jednotliví klienti by se však měli vyvarovat například vyhazování zásilky s vyznačeným PINem do běžného odpadu nebo do kontejneru na separovaný odpad. Všechny dokumenty s důležitými údaji je potřeba před vyhozením znehodnotit tak, aby údaje již nebyly čitelné – například roztrháním na drobné kousky nebo zamalováním černým fixem.

Prostá krádež

Je to nejjednodušší způsob zneužití karty. Do doby zjištění ztráty a následné blokace karty má zloděj šanci získat finanční prostředky buď zadáním PIN, pokud ho zná, nebo neoprávněnou platbou u obchodníka (pokud není karta chráněna čipem) či na Internetu. Při placení u obchodníka bez zadání PINu je povinností obchodníka kontrolovat shodu podpisů na stvrzence a rubu platební karty. Zdařilou napodobeninou podpisu však obchodník nemusí rozpoznat. V případě, že je transakce provedena bez řádného souhlasu klienta, jedná se o neautorizovanou transakci.

Ztráty ze zneužití platební karty lze minimalizovat především obezřetností – tedy opatrným nakládáním jak s platební kartou, tak identifikačními údaji k ní. Pomocí předejít škodám může i pojištění proti zneužití karty.

Text byl převzat ze studie Podvody v oblasti bezhotovostních plateb v ČR autorů Dr. Ing. Františka Klufy a JUDr. Petra Scholze, Ph.D. Text byl redakčně upraven.

Kontaktní údaje

Kancelář finančního arbitra

Legerova 69
110 00 Praha 1

Tel.: + 420 257 042 094

Fax.: + 420 257 042 089

E-mail: arbitr@finarbitr.cz

ID datové schránky: qr9ab9x

www.finarbitr.cz

www.financniarbitr.cz

www.financniombudsman.cz

Kontakt pro média:

Ing. Běla Fialová

fialova@finarbitr.cz, tel. 257 042 093

Úřední hodiny:

Pondělí - Čtvrtek od 8:30 hod. do 15:30 hod.

Pátek - od 8:30 hod. do 14:30 hod.

