platebních karet, aby svůj občanský průkaz předložili, pokud o to budou obchodníkem požádáni.
V praxi se ukazuje, že jde o velmi účinnou metodu, jak zabránit zneužívání platebních karet. Ve spolupráci bank, obchodníků a Policie ČR bylo zadrženo několik pachatelů právě díky žádosti obchodníka o průkaz totožnosti.

12. Je důležité uchovávat prodejní doklady při platbě kartou u obchodníka?

Ano, doporučujeme alespoň po dobu 3 - 6 měsíců prodejní doklady uschovávat. Držitel platební karty může použít tyto prodejní doklady jak ke kontrole transakcí na výpisu z účtu, tak v případě zjištění nesrovnalostí nebo při případném reklamačním řízení. Viz dále.

13. Jak má klient postupovat v případě, že na výpisu ze svého účtu nalezl transakce, které neprovedl?

Doporučujeme všem spotřebitelům (klientům bank), aby pozorně kontrolovali pravidelný měsíční výpis transakcí provedených platební kartou a ujistili se, že obsahuje pouze transakce provedené jejich platební kartou, a ve výši, která odpovídá skutečnosti. Při jakékoli nesrovnalosti je nutné neprodleně informovat banku a požádat o prověření transakce. Pokud klient může reklamaci čímkoli doložit (např. karta byla použita v zemi, kterou klient sice navštívil, ale v době transakce byl již mimo tento stát a může to doložit např. razítkem v cestovním pasu nebo letenkou/jízdenkou), doporučujeme takovéto doklady ihned předložit - šetření se tím urychlí.

14. Na co je třeba dávat pozor při placení kartou na internetu, při poštovní či telefonické objednávce? Existuje více způsobů plateb bez tzv. přítomnosti karty?

Existují dva způsoby platby bez přítomnosti karty:
- tzv. MO/TO transakce
- platby po Internetu

Při poštovní nebo telefonické objednávce (MO/TO) je nutná maximální obezřetnost - v případě jakýchkoli pochybností o obchodníkovi doporučujeme klientům zvolit jiný způsob úhrady, než platební kartou.
Při platbě po internetu je vhodné se přesvědčit, že komunikace mezi uživatelem (držitelem platební karty) a internetovým obchodem je zabezpečena - tzv. kryptována. Zda a jak je komunikace zabezpečena, by měl mít obchodník uvedeno na svých stránkách. Za dostatečné zabezpečení se považuje protokol SSL. Nejvyšší úroveň zabezpečení nabízí protokol 3D – secure, který je u obchodníků prezentován pod ochrannou známkou Verified by VISA nebo MasterCard Secure Code. V případě jakýchkoli pochybností o důvěryhodnosti obchodníka však opět doporučujeme klientům zvolit jiný způsob úhrady než platební kartou.
Vždy platí zásada poskytnout číslo karty pouze důvěryhodným partnerům.

3. Co dělat v případě, že se staneme obětí podvodu?

Co má držitel platební karty udělat v případě, že mu byla **karta zcizena nebo kartu ztratil**, nebo se **cizí osoba dostala k informaci o PINu?**
Držitel karty je obvykle podle Obchodních podmínek pro vydávání a používání debetních, kreditních a charge karet k účtu vedenému jeho bankou, povinen neprodleně ohlásit ztrátu, odcizení, příp. možnost zneužití karty neoprávněnou osobou. Je to ostatně i v jeho zájmu. **Kontaktujte tedy v takovém případě bezodkladně svoji banku!**
Co má uživatel účtu udělat v případě, že si uvědomí, že **poskytl cizí osobě důvěrné informace ohledně elektronického přístupu k jeho účtu (phishing aj.)?**
Držitel karty je obvykle podle Obchodních podmínek pro zřízení a vedení účtu jeho bankou povinen neprodleně ohlásit takovou situaci. Je to ostatně i v jeho zájmu. **Kontaktujte tedy v takovém případě bezodkladně svoji banku!**

a. Česká spořitelna

Centrála České spořitelny, a.s. , Olbrachtova 1929/62, 140 00 Praha 4, tel: 261 071 111
Informační linka České spořitelny: 800207207
Dotazy a připomínky k jednotlivým produktům nebo obecné povahy zasílejte e-mailem na adresu: csas@csas.cz

Linka SERVIS 24:

tuzemská - pevná	844 111 144
Telefónica O2	726 111 144
T-Mobile	605 661 144
Vodafone	776 991 144
ze zahraničí	+420 582 405 405
e-mail:	servis24@csas.cz

b. ČSOB

Ústředí ČSOB: Radlická 333/150, 150 57 Praha 5,
Telefon 224 111 111, E-mail Info@csob.cz
Infolinka (zelená linka) - obecné informace

Telefon	800 300 300
T-Mobile	603 676 676
O2	729 933 933
Vodafone	776 992 992
E-mail	Info@csob.cz

GE Money Bank

Operátor nonstop tel.: 224 443 636

Komerční banka

Centrála KOMERČNÍ BANKY, Na Příkopě 33, 114 07 Praha 1, P.O. BOX 839, Česká Republika
Informační linka Komerční banky:
800 111 055; +420 485 262 800 (pro volání ze zahraničí)
Expresní linka Komerční banky:
800 111 124; + 420 485 262 124 (pro volání ze zahraničí)

mBank

Korespondenční adresa: mBank, retailové bankovnictví BRE Bank S.A., P.O. Box 366, 111 21 Praha 1.
Centrála: Nile House, Karolinská 654/2, 186 00 Praha 8
Pokud nemáte přístup k internetu a potřebujete rychle provést platbu, zjistit nastavení služeb nebo zjistit potřebné informace, můžete využít služeb mLinky. Operátoři jsou vám k dispozici od 7 do 22 hodin (v pracovní dny) pro provádění všech typů operací;
Informační servis, objednávání produktů a blokace platebních karet funguje 24 hodin denně. Volejte přímo na číslo: 844 777 000.
Pokud jste v zahraničí nebo je pro vás výhodnější pevná linka, volejte na číslo: +420 246 017 777.

Raiffeisenbank a.s.

Sídlo/centrála: Hvězdova 1716/2b, 140 78 Praha 4
Telefon: 225 541 111, Fax: 225 542 111
Nepřetržitá bezplatná telefonní linka: 800 900 900
Ze zahraničí: + 420 417 941 444 (cena hovoru dle tarifu Vašeho operátora)
Nonstop hotline linka: 800 900 000 - telefonní linka při ztrátě, odcizení nebo zneužití platební karty.
Ze zahraničí:: + 420 417 941 446 (cena hovoru dle tarifu Vašeho operátora)
Vaše nápady a připomínky zasílejte na: info@rb.cz,
Internetová adresa: www.rb.cz

KonzumentTest, číslo 8, květen 2009; © Sdružení českých spotřebitelů, 2008

ISSN 1801-528X

Toto vydání **KonzumentTest** bylo připraveno z informací ze Studie podvodů v oblasti bezhotovostních plateb v ČR (Klufa, Scholz) a z webových stránek bank; k tisku zpracoval a upravil Ing. L. Dupal.

Navštivte nás na takto označených místech po celé ČR:

Kontaktní místo

Kontaktní místo:
Sdružení českých spotřebitelů, o.s.
Budějovická 73, 140 00 Praha 4, tel/fax: 261263574/261262268,
e-mail: spotrebitel@regio.cz; **www.konzument.cz**

Prostřednictvím španělské organizace ADICAE je projekt financován Evropskou unií. Spolufinancování realizace české části projektu poskytla Česká spořitelna, a.s. SČS děkuje.

Konzument test

Občasník Sdružení českých spotřebitelů
Číslo 8 / květen 2009

Úvod

Prevence proti podvodům při nehotovostních platbách

Operace s bankomaty, platby a převody peněz přes internet. Jak se bránit podvodům?

„Problém podvodů při bezhotovostních platbách v Evropě je v současnosti spojen s existencí dobře organizovaných skupin, jejichž aktivity jsou přeshraniční. Evropská komise proto vyjadřuje požadavek, aby se všechny zainteresované strany podílely na řešení problému; je třeba bojovat skupinově v mnoha členských státech proti tomuto druhu podvodného jednání.“

Sdružení českých spotřebitelů (SČS) se podílí na realizaci evropského projektu zaměřeného na prevenci podvodů při nehotovostních platbách. Projekt, do něhož jsou zapojeny spotřebitelské organizace z několika zemí EU, je dotovaný Evropskou komisí a je jednou z možností jak naplňovat výše citovaný záměr. **Koordinátorem realizace** je španělská spotřebitelská organizace, specializující se na bankovní služby **ADICAE (Asoción de Usuarios de Bancos, Cajas y Seguros)**. Partnery jsou spotřebitelské organizace kromě Česka z dalších zemí – ze Slovenska, Slovinska, Rumunska, Litvy, Itálie a Bulharska.
KonzumentTest věnovaný tomuto tématu je jedním z více výstupů projektu, tzv. technický katalog podvodů. Má zájemcům podat souhrn informací o nejdůležitějších podvodných praktikách při platbách kartami, při internetových platbách a převodech a při operacích s bankomaty (ATM). Spotřebitelé zde naleznou nejen základní rady, jak předcházet podvodům při bezhotovostních platbách, ale také jaké kroky podniknout, pokud se obětí podvodného jednání stanou anebo mají podezření, že se tak stalo.
Doporučujeme se též obrátit na speciálně zřízené stránky www.prevencepodvodu.cz.

1. Obvyklé podvodné praktiky při nehotovostních platbách

Nové technologie a nové způsoby plateb přinášejí i nové způsoby podvodných praktik. Tento text je pouze stručným shrnutím informací. Více se lze dočíst v podrobnějších zdrojích, např. ve studii o podvodech (viz *www.prevencepodvodu.cz)*.

a. Technické členění podvodů

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. Ta se nezdaří, klient odchází bez karty, kterou podvodník následně vytáhne zpět a zneužije ji, než dojde k její blokaci. Proti tomuto způsobu dnes většinou existuje účinná obrana, kterou banky implementovaly na bankomaty, v podobě dodatečným ochranných adaptérů.
Skrytá kamera – Pomocí malé skryté kamery podvodník zjišťuje PIN, často je 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, CVCV 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 – Je to poměrně vzácný způsob získání PINu spočívá v instalaci senzorů na klávesnici bankomatu nebo např. na vstupní dveře do samoobslužné zóny. Opět je jeho účelem získat PIN. Může být kombinován s účelovou krádeží, přepadením nebo jiným způsobem, jak se zadrží karta 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 rovněž 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. kódu 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 důvěřivost lidského prvku; dochází při ní k zneužití emailové pošty s cílem získání identifikačních údajů; riziko spočívá v tom, že zpravidla do e-mailového formuláře vyplníte číslo své platební karty s dalšími osobními údaji; e-mail, který se jeví, že byl doručen bankovní institucí, však je podvodný, a pokud dojde k zadání k těchto citlivých dat, může dojít v krátkém časovém sledu k výrobě padělku platební karty a k jejímu zneužití - během několika minut může dojít k výběrům z bankomatu v zahraničí.
Pharming – První podoba pharmingu je sice efektivní, ale pro podvodníka, který chce jejím prostřednictvím získat citlivé údaje, značně obtížná. Spočívá v tom, že klient zadá ve svém internetovém prohlížeči nějakou adresu. Nedojde ale k jejímu překladu na správnou adresu, ale na adresu, kterou zadali podvodníci. Spojení s bankou je přesměrováno na jiný kanál, jehož www stránky, připravené podvodníky, jsou velice podobné oficiálním stránkám klientovy banky. Při přihlášení klienta ke komunikaci s bankou získají podvodníci citlivé údaje a bude následovat odčerpání finančních prostředků s klientova účtu.
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 jednotlivé počítače. 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? Je jich více, jenom náznakově je v zásadě je můžeme 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 samotném klientovi, který s počítačem pracuje a lze je velice stručně shrnout pod výraz obezřetnost, obezřetnost a zase obezřetnost. Znamená to nestahovat z internetu neznámé aplikace, otevírat odkazy v e-mailech apod.

Spoofing – Je to technika, která není v České republice dosud rozšířena. Spoofing znamená doslova napálit, převézt, vodit 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 lokálních sítí mohou být za určitých podmínek zjištěna citlivá data, která mohou být následně zneužita.

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 zabezpečte nějak odvoz a skladování „odpadních informací“, a to jak ve fyzické, tak i v elektronické podobě.

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 chipem). Povinností obchodníka je však kontrolovat shodu podpisů na stvrzence a rubu platební karty. V případě, že je transakce provedena bez řádné identifikace klienta, jedná se o neoprávněnou transakci. Ztráty lze minimalizovat pojištěním proti zneužití.

b. Transakční členění podvodů

Zneužití držitelem karty – Jedná se o úmyslné provedení platební transakce nebo výběru v bankomatu s jejím následným popřením; tyto podvody nejsou časté, ale dochází k nim; držitel karty a v tomto případě i podvodník se však tímto vystavuje riziku trestního postihu.

Zneužití osobou blízkou – Jedná se o provedení neoprávněné platební transakce nebo výběru v bankomatu blízkými příbuznými, dětmi, přáteli, spolupracovníky. Zjistit údaje o platební kartě je pro ně někdy velmi snadné a zneužití platební karty pak jednoduché.

Zneužití osobou cizí – K tomuto zneužití dochází především při zcizení nebo ztrátě platební karty; ke zneužití osobou cizí však dochází i při transakcích, kdy se jedná o součinnost podvodníka a podvedené osoby; mezi rizikovou skupinu patří především starší občané, kteří si někdy nevědí rady s obsluhou bankomatu nebo platbou a nabídne se „pomocník“, který jim pomůže např. s výběrem hotovosti a výsledkem je mnohdy neoprávněný výběr nebo zneužití citlivých údajů z platební karty.

Zneužití nedoručené karty - Většina bank zasílá platební karty svým klientům poštou v oddělené zásilce od PIN. Některé takto doručované karty a PIN však mohou být vlivem „nesprávného doručení“ zneužity. Znám je případ, kdy doručení zasílané platební karty a následně PINu pro prarodiče bylo převzato vnukem a došlo k následnému zneužití této karty. Posouzení odpovědnosti za doručení zásilky pak podléhalo správnímu orgánu. Tento podvod není však masově rozšířen.

Platby na dálku – Jedná se o použití elektronického platebního prostředku na dálku bez jeho fyzického předložení; podstatou podvodu je zneužití citlivých údajů jako je jméno držitele karty, čísla karty a doby platnosti karty platbou na internetu; §18 zákona o platebním styku však stanovuje že, „prohlásí-li držitel, že tento elektronický platební prostředek neužil, má právo požadovat od vydavatele neprodlené vrácení“; tímto je držitel karty velmi dobře chráněn před zneužitím před takovými platebními transakcemi.

Podvodná žádost o kartu – Nejedná se o rozšířený podvod v České republice; podstatou podvodu je předložení podvodné žádosti o vydání platební karty pro jinou osobu, než která je oprávněna nakládat s účtem, bezpečností postupy v bankách tomuto typu podvodu zabraňují.

Zneužití obchodníkem – U tohoto podvodu je jedná o neoprávněné provádění opravných transakcí bez souhlasu držitele platební karty; některé typy obchodů, jako např. hotely a autopůjčovny, mají oprávnění tyto dodatečné opravné transakce provádět (např. za nenahlášenou útratu za minibar v hotelu nebo za poškození vypůjčeného vozidla); z důvodu toho, že však je tato transakce ovlivněna lidským faktorem, tj. osobou, která tuto dodatečnou opravnou transakci provádí, může dojít k uskutečnění neoprávněné transakce, následná reklamace u banky bývá povětšinou úspěšná, ale přesto je však získání peněžních prostředků zpět omezeno časovou lhůtou pro řešení reklamace; další možností zneužití obchodníkem je, že může po provedení platební transakce např. v restauraci dojít k vrácení jiné platební karty a originál může být následně zneužit.

2. Obranné a preventivní prostředky

Při bezhotovostních platbách se spotřebitelé často chovají velmi neopatrně, až naivně, či nezodpovědně. Asi bychom na ulici neznámé osobě nedali do rukou svou peněženku s hotovostí, aby nám šla koupit noviny, než si vykouříme cigaretu či dočteme noviny. Při bezhotovostním platbách se však takto někdy chováme, a všanc přitom dáváme mnohem větší obnosy.

V následujícím se pokusíme shrnout nejzákladnější preventivní opatření, jejich dodržování nám pomůže vyvarovat se, abychom se stali obětmi podvodů. Rady členíme na část elektronických plateb a převodů a na část zaměřenou na operace s bankomaty (ATM).

a. Rady pro zajištění bezpečnosti pro e-banking

1. Sledujte aktuální informace své banky

Každá banka zveřejňuje informace k bezpečnostní situaci na svých internetových stránkách. Zde najdete aktuální upozornění a doporučení, která Vám pomohou používat danou aplikaci bezpečně.

2. Nastavení počítače pro e-banking, pravidelná aktualizace

Věnujte pozornost nastavení svého počítače při využívání PŘÍMÉHO BANKOVNICTVÍ, zejména při prvním přihlášení, ale i později, průběžně.

Banky obvykle pro ověření správného nastavení Vašeho počítače nabízí využít jednoduchý test. Test vypíše případné požadavky na změnu ve Vašem počítači (např. ikona „Otestujte si svůj počítač“, nebo podobně).

Vhodné nastavení svého počítače můžete provést také samostatně v následujících několika krocích:

1. krok - Zařaďte server své banky mezi důvěryhodné servery;
2. krok - Nainstalujte si příslušný vyžadovaný operační systém (např. Java Virtual Machine);
3. krok - Nastavte použití příslušného vyžadovaného operačního systému (např. Java Virtual Machine) v prohlížeči;
4. krok - Povolte použití „cookies“ pro server Vaší banky; popř. další.

Pravidelně instalujte aktualizační soubory, které odstraňují některé jeho chyby a omezují bezpečnostní rizika. Doporučujeme Vám zapnout automatickou aktualizaci systému Windows. Na adrese http://www.microsoft.com/cze/security/protect/ jsou také popsány základní kroky k zabezpečení Vašeho systému.

3. Chraňte svůj osobní certifikát

Pokud máte přístup ke svému účtu založen na osobním certifikátu, pamatujte, že tento nahrazuje Váš vlastnoruční podpis a je tedy „přístupovým klíčem“ k Vašim účtům a financím. Proto chraňte svůj osobní certifikát proti zneužití třetími osobami. Doporučuje se uchovávat osobní certifikát na přenosném médiu (např. na USB disku, disketě nebo CD) a tyto nosiče mít pod kontrolou na bezpečném místě. Některé banky pro zvýšení bezpečnosti uložení osobního certifikátu nabízí využití čipové karty.

4. Nepoužívejte jednoduché heslo / PIN

Jednoduché heslo nebo PIN lze snadněji zachytit, rozluštit a zneužít. Nepoužívejte proto slova a čísla, která mají souvislost se jmény rodinných příslušníků, jejich datem narození, jejich telefonním číslem, apod. U hesla doporučujeme zvolit kombinaci velkých a malých písmen, číslic a speciálních znaků (tečka, vykřičník, otazník atd.). Heslo by mělo mít minimálně osm znaků.

Banky doporučují volit odlišný PIN k čipové kartě od ostatních PINů.

5. Chraňte svoje bezpečnostní údaje

Heslo nebo PIN si nezaznamenávejte na poznámkové papírky, do diářů, do telefonů, na čipovou kartu apod. V žádném nastavení počítače nepovolujte zapamatování hesel.

Dodržujte zásadu, že hesla se nikomu nesdělují, a to ani rodinným příslušníkům! Doporučujeme, abyste si svá hesla a PINy po určitých časových intervalech měnili.

6. Nastavte si zasílání zpráv

Doporučujeme Vám nastavit si zasílání zpráv (SMS nebo e-mail), které Vás budou informovat o veškerých platbách provedených z Vašeho účtu nebo platební karty.

7. Používejte svůj počítač, nepracujte na neznámém počítači

K využívání služeb přímého bankovnictví doporučujeme používat pouze svůj domácí, příp. osobní firemní počítač. Neumožňujte práci s Vaším počítačem neznámé osobě. Před každým odchodem od počítače použijte CTRL+ALT+DEL pro uzamknutí počítače, nebo u starších operačních systémů si aktivujte spořič obrazovky chráněný heslem. Nepřihlašujte se k internetu, pokud jste k počítači přihlášeni s administrátorskými právy, tj. s právy provádět instalace programů.

K využívání služeb přímého bankovnictví nedoporučujeme používat počítač, o kterém nic nevíte (např. počítač v internetové kavárně).

8. Používejte aktuální antivirový program/y

Vždy mějte na svém počítači nainstalovaný antivirový program, který zvyšuje ochranu před škodlivými programy - viry. Stejně tak je vhodné používat anti-spyware program (např. Ad-aware, Spybot), který zvyšuje ochranu před sledováním Vaší činnosti na PC pomocí parazitních programů. Antivirový a anti-spyware program pravidelně aktualizujte.

K minimalizaci rizika neoprávněného přístupu na Váš počítač při připojení k internetu slouží tzv. firewall. Jedná se o ochranný program nebo technické zařízení, které zpracovává pouze Vámi zadané dotazy do sítě internet a všechna ostatní příchozí (potencionálně nebezpečná) data odfiltruje. Sledujte rady a doporučení své banky.

9. Nenavštěvujte neznámé stránky a nestahujte z internetu neznámé soubory

Navštěvujte na internetu pouze známé a důvěryhodné stránky. Vyvarujte se stahování neznámých souborů z internetu na Váš počítač, které mohou společně se svým původním účelem nainstalovat i nebezpečné programy. Zejména stránky s erotickým obsahem, nelegálním software obsahují spyware a viry, které mohou infikovat Váš počítač a následně provádět činnost, kterou nemáte pod kontrolou.

10. Otvírejte pouze důvěryhodné e-maily, nereagujte na podvodné e-maily

Neotvírejte e-mailové zprávy od adresátů, které neznáte nebo zprávy, které mají podezřelý název či obsah. Nespouštějte přílohy ani odkazy takovéto e-mailové zprávy a zprávu bez otevření smažte.

Nesdělujte osobní údaje, hesla či kódy PIN formou e-mailu. Žádná banka tyto údaje nikdy nepožaduje.

Žádná banka nikdy neoslovuje klienty v otázkách bezpečnosti e-mailem.a nezasílá nevyžádané e-maily s odkazy na internetové adresy. V případě, že obdržíte nevyžádaný e-mail obsahující internetový odkaz na stránky „Vaší“ banky, na e-mail nereagujte a na odkaz ani neklikejte!

11. Kontrolujte na přihlašovací stránce řádek pro zadání internetové adresy.

Vždy se přesvědčte, že se jedná opravdu o stránku, kterou požadujete zobrazit. Před samotným přihlášením pokleplejte na ikonu zámku buď v pravé dolní části okna prohlížeče Internet Explorer 6, nebo vedle řádku pro zadání internetové adresy v Internet Exploreru 7, a ověřte, že certifikát zabezpečující připojení byl vydán pro vámi zvolenou adresu.

12. Kontaktujte svoji banku

Pokud při přihlašování nebo práci s bankovním účtem prostřednictvím internetového bankovnictví budete mít jakékoliv pochybnosti, kontaktujte prosím neprodleně klientskou podporu své banky (viz dále).

b. Rady pro zajištění bezpečnosti pro platební karty

1. V čem spočívá bezpečnost čipových karet?

➡ Ve způsobu ověření držitele při platbách kartou. Pokud budete platit čipovou kartou u obchodníka, který akceptuje čip, budete vyzváni k zadání PIN. Ve srovnání s ověřením prostřednictvím podpisu u karet s magnetickým proužkem, je ověření prostředním PIN bezpečnější. Hodnotu PIN má k dispozici pouze držitel karty na rozdíl od podpisu, který je viditelně zaznamenán na zadní straně karty.

➡ V bezpečnosti uložení dat v čipu a kontrolovaném přístupu k těmto datům. Data uložená v čipu jsou dostatečně chráněna a karty tak významně přispívají ke snížení rizika podvodných transakcí. Údaje, které jsou uloženy přímo v čipu jsou chráněny vysokou úrovní šifrování. Čip není možné snadno okopírovat jako magnetický proužek (tzv. skimming), respektive bez znalosti přístupových klíčů není možné zaznamenané údaje na čipu přečíst.

2. Podepisování platební karty (viz podpisový proužek na zadní straně karty)

V případě karty, která je vybavena pouze magnetickým proužkem, je držitel ověřen podepsáním prodejního dokladu. Tato karta musí být držitelem bezpodmínečně podepsána. Při převzetí doporučujeme klientům pořídit si kopii zadní strany karty s podepsaným podpisovým proužkem, nebo o to požádat pracovníky pobočky České spořitelny. Tím klient předejde mnoha problémům v případě ztráty či odcizení karty (reklamační řízení – nesouhlas podpisu).

Je v zájmu klienta, aby ihned po převzetí podepsal i čipovou kartu. Čipové karty mají kromě čipu, který je umístěn na přední straně karty, i magnetický proužek. Pokud budete platit čipovou kartou u obchodníka, který doposud není vybaven čipovou technologií, proběhne transakce na magnetický proužek. V tomto případě bude držitel ověřen podepsáním prodejního dokladu. (V případě, že obchodník je vybaven čipovou technologií, probíhá transakce na čip na základě zadání PINu držitelem karty).

3. Sdělování PIN při platebních operacích

Ověření klienta PINem v případě čipové transakce probíhá pouze u transakcí, u kterých je fyzicky přítomna platební karta, tj. platba kartou u obchodníků v „kamenných“ obchodech nebo výběr hotovosti.

Případně můžete být vyzváni k zadání PIN a podpisu současně (karty MAESTRO). Doporučujeme klientům, aby své PIN zadávali vždy diskrétně tak, aby jej jiná osoba nemohla vidět, a jen tehdy, když jsou k jeho zadání vyzváni hlášením na displeji terminálu či PIN padu (zařízení k zadávání PIN).

Pokud držitel čipové karty provádí transakci bez fyzické přítomnosti karty (např. platba kartou na internetu), bude probíhat ověření klienta stejně jako v případě karty s magnetickým proužkem. **V žádném případě při e-bankingu neuvádí klient PIN!** Podle typu obchodníka může být držitel požádán o uvedení:

➡ čísla platební karty;
➡ platnosti platební karty;
➡ CVV2 (karty VE a Visa)/CVC2(karty MasterCard) kódu.

Dále platí, že žádná kartová společnost (asociace) ani banka vydávající platební karty nikdy nevyžadují po klientovi poskytnutí důvěrných informací o bankovním spojení a o platební kartě, včetně kódu PIN. Pokud by klient takový „podvržený“ dotazník vyplnil, vystavuje se riziku, že jeho data budou zneužita, a to zejména prostřednictvím elektronických nákupů nebo budou použita k výrobě kopie (padělku) jeho platební karty. V žádném případě tedy klient nemá na pokusy, kdy je k poskytnutí takových důvěrných informací vyzýván, reagovat jiným způsobem, než že informaci co nejdříve předá své bance.

4. Sdělování PIN jiným osobám

PIN kód je nutné zachovávat v tajnosti. Smí jej znát pouze majitel platební karty. Karta je nepřenosná a je určena pouze pro potřebu klienta, na jehož jméno byla vystavena. Kartu nelze půjčovat k nákupům či dokonce výběrům hotovosti (prozrazením PIN kódu dojde k porušení smluvních podmínek, které klient podepisuje při převzetí karty), a to ani členům rodiny.

PIN kód by si držitel platební karty neměl v žádném případě poznamenávat či jej zapisovat na platební kartu. V případě odcizení či ztráty platební karty pak mají podvodníci k dispozici vše, co je pro použití platební karty třeba.

5. Zapomenutí PINu

V případě, že klient zapomene PIN ke své platební kartě, řídí se konkrétními Obchodními podmínkami; obvykle může na kterékoli pobočce své banky zažádat o znovuzaslání PINu. Žádost může být také podána prostřednictvím telefonické služby, má-li tuto službu klient ke svému účtu sjednanou. Znovuzaslání PINu bývá zpoplatněno dle platného sazebníku příslušné banky.

6. Jaké hodnoty použít při změně PIN?

Pokud banka pro Vaši kartu umožňuje změnu PIN kódu, volbu pro změnu PIN naleznete v nabídce „Služby“ v kterémkoliv bankomatu Vaší banky. Při změně PIN Vám doporučujeme se řídit následujícími bezpečnostními pravidly:

➡ nezadávat čtyřčíslí ze stejných čísel;
➡ nezadávat část data narození držitele nebo rodinných příslušníků;
➡ nezadávat část čísla karty nebo jiné číselné údaje, které lze jednoduše zjistit.

7. Jak správně zacházet s platební kartou?

Doporučujeme platební karty nosit odděleně od osobních dokladů a finanční hotovosti.

8. Znehodnocení magnetického proužku platebních karet

Magnetický proužek platební karty může být za určitých okolností poškozen či znehodnocen. Proto je nutné údaje na magnetickém proužku karty chránit před tepelným a mechanickým poškozením (poškrábání, odření) a před působením vnějších magnetických polí (ke zmagnetizování může dojít např. mobilním telefonem, magnetickým zapínáním kabelek, elektromotory, počítači atd.).

9. Pravidla pro předcházení zneužití karty při výběru hotovosti v bankomatech

➡ Vyberte si bankomat, který znáte, nebo, pokud ho neznáte, doporučujeme použít bankomat v dobře osvětleném a bezpečném místě.
➡ Neprovádějte raději výběr, pokud se v okolí bankomatu pohybují lidé, kteří Vám připadají podezřelí - výběr hotovosti z bankomatu je nezbytné provádět bez asistence cizí osoby; vyžadujte, aby lidé, kteří stojí v řadě za Vámi, dodržovali od Vás dostatečný odstup, aby neměli možnost pozorovat, jaké pokyny, čísla, částky na bankomatu zadáváte;

➡ Za žádných okolností nesmí klienta při uskutečňování transakce rušit neznámá osoba (i kdyby tvrdila, že je pracovníkem banky, bezpečnostní služby nebo Policie ČR apod.); pracovníci, kteří bankomaty doplňují či udržují, nemají žádný důvod přerušovat transakci a také to nikdy nedělají;
➡ Při zadávání PIN kódu do bankomatu je nutné se ubezpečit, že nikdo nemá možnost jej odezírat, při zadávání PINu doporučujeme zakrýt klávesnici volnou rukou;
➡ PIN je třeba zadávat pouze na klávesnici bankomatu, nikdy ne na zařízení u vstupních dveří samoobslužné zóny, kde je bankomat umístěn;
➡ Doporučujeme, aby se držitel platební karty před výběrem hotovosti z bankomatu ubezpečil, že vstupní otvor pro vložení karty nenese známky manipulace nebo poškození;
➡ Nikdy netlačte násilně svou kartu do štěrbiny bankomatu;
➡ Pokud bude platební karta z jakéhokoliv důvodu zadržena bankomatem a nebude vydána o jejím zadržení potvrzenka, doporučujeme ihned kontaktovat svoji banku a kartu zablokovat. Pokud se Vám zdá, že bankomat nepracuje správně, transakci stornujte a vyčkejte na vydání své karty. Danou skutečnost nahlaste bance;
➡ Nespěchejte při transakci, v klidu uložte svou hotovost i kartu do peněženky před tím, než odejdete od bankomatu.

10. Pravidla pro předcházení zneužití karty při placení u obchodníků

➡ Vždy je třeba pečlivě zkontrolovat na prodejním dokladu a dokladu o zaplacení platební kartou datum, částku, označení prodejny; proškrtnutnout všechna volná místa před sumou a mezi řádky a nikdy nepodepisovat nevyplněné prodejní doklady (tj. zejména v případě, kdy budou údaje z platební karty klienta sejmuty za použití tzv. imprinteru - mechanického přístroje pro sejmutí dat z karty);
➡ Je třeba dávat pozor, zda personál prodejny neodchází s kartou do zázemí nebo s ní nemanipuluje nezvyklým způsobem;
➡ Pokud dojde k situaci, kdy obchodník klientovi kartu odnese a posléze sdělí, že transakci nebylo možné uskutečnit, je nutné poznamenat si toto prodejní místo a v případě, že klient zaplatí v hotovosti, doporučujeme uschovat tento doklad o zaplacení pro eventuelní reklamaci (pokud by se transakce z tohoto prodejního místa objevila na výpisu držitele karty);
➡ Účtenky je nutné uschovat pro případné reklamace;
➡ Vždy je nutné zkontrolovat, zda platební karta, kterou personál klientovi vrátí, je opravdu jeho.

11. Může obchodník při placení kartou v některých případech požadovat předložení občanského průkazu klienta?

Obchodník předloženým občanským průkazem ověřuje - na základě žádosti smluvní banky - totožnost klienta. Protože tímto způsobem může zabránit podvodu, a tím také eventuální finanční ztrátě, doporučujeme držitelům