Beata Dobiašová

Ochrana osôb pred podvodmi v elektronickom bankovníctve

Anotácia: Článok sa zameriava na význam používania informačných a komunikačných technológií v oblasti elektronického bankovníctva. Poukazuje na formy elektronického bankovníctva, jeho výhody pre klienta, ako aj pre banku. Súčasne sa zameriava na riziká, ktoré postihujú oblasť elektronického bankovníctva. Poukazuje na druhy najviac používaných podvodov a v druhej časti sa zameriava na pravidlá a postupy bezpečného používania elektronického bankovníctva.

Kľúčové slová: elektronické bankovníctvo, internetbanking, platobné karty, phishing, pharming, trójske kone, skimming, card-trapping, podvody.

Používanie informačných a komunikačných technológií celosvetovo rastie obrovským tempom. Spoločnosť je dnes už celkom závislá od ICT[1] a je prirodzene vystavená útokom vedeným do tejto oblasti. Medzi dôležité oblasti, ktorých sa kybernetická kriminalita dotýka, je široká oblasť moderných telekomunikačných technológií[2]. Svet telekomunikácií založený na moderných technológiách má v dnešnom svete svoj nezastupiteľný význam, ale zároveň skrýva rozmanitú škálu rôznych rizík. Tieto riziká je možné triediť tak z technologického uhla pohľadu, ako aj z uhla trestnoprávneho pohľadu.

Kriminalita páchaná v prostredí hight-techniky, teda v prostredí, v ktorom podľa vykonanej analýzy a názorov expertov nás v súčasnosti i v budúcnosti očakáva široká škála hrozieb spojených s páchaním závažnej trestnej činnosti.[3]

Vzhľadom na uvedené skutočnosti je pochopiteľné, že riziká postihujú aj oblasť elektronického bankovníctva, ktoré moderné telekomunikačné technológie využíva v širokom rozsahu.

Slovenské banky síce majú zabezpečenie svojho internetového bankovníctva na vysokej úrovni, aj vďaka ústretovému prístupu svojich klientov, ktorí uprednostňujú bezpečnosť pred pohodlím. Medzi veličinami bezpečnosť a pohodlie platí nepriama úmera – čím je vyššia bezpečnosť, tým je pohodlie klienta pri prihlasovaní a vykonávaní zabezpečených operácií nižšie.[4] Banky kombinujú známe prvky zabezpečenia prístupu na účet klienta prostredníctvom internetu rôznym spôsobom, od voľných kombinácií s maximálnym pohodlím až po prekombinované s množstvom bezpečnostných prvkov – od PIN po čipovú prihlasovaciu kartu.

Formy elektronického bankovníctva:

- Telefónbanking (Phonebanking)[5]

---

[1] ICT – Information and Communication Technologies.

[2] TUREČEK, J. et. al. *Policejní technika*. Vydavatelstvía nakladatelství Aleš Čeněk, Plzeň 2008, s. 198 -210. ISBN 978-80-7380-119-9.

[3] KUMMER, R , TALLO, A. Kriminalita v oblasti moderní telekomunikační techniky I. In *Policajná teória a prax, roč. XV., č. 3, 2007, s. 73 – 81*.

[4] Aj keď sa elektronické bankovníctvo teší vysokej popularite a čoraz viac narastá počet ľudí, ktorí využívajú prínosy a výhody internetového bankovníctva. Výskum uskutočnený spoločnosťou Forrester Research na vzorke 23 000 Európanov ukázal, že viac ako 40 percent všetkých európskych používateľov sa neodváži riešiť svoje záležitosti s bankami cez internet.

[5] Dve formy phonebankingu:Interactive Voice Responcer (IVR) – interaktívny hlasový odpovedač - automat dokáže komunikovať pomocou hlasu s klientom a vykonávať ním zadané príkazy, Call Centrum- komunikáciu cez telefón sprostredkúva operátor a vykonáva operácie s podporou bankového informačného systému podobne ako pracovník za okienkom,
Niektoré banky do phonebankingu zahŕňajú aj použitie faxu, prostredníctvom ktorého zasielajú napr. výpisy z účtov.

- GSM-banking (SMS)
- Internetbanking
- E-mailbanking
- WAP-banking[6]
- Homebanking[7]
- Platobné karty
- Iné.

Elektronické bankovníctvo prináša pre klienta aj pre banku celý rad výhod. Výhody elektronického bankovníctva pre klienta sú najmä:

- možnosť pracovať s účtami v pohodlí kancelárie, doma, ale aj na cestách nielen na Slovensku, ale aj v iných krajinách, všade, kde je možný prístup k telefónu a internetu,
- elektronické bankovníctvo je prístupné 24 hodín denne, 7 dní v týždni, takže klient môže vykonávať svoje bankové operácie, aj keď je banka zatvorená,
- úspora času a finančných prostriedkov, pretože klient nemusí ísť do banky, čo ho stojí čas a peniaze za dopravu,
- pomocou e-bankingu sa dajú zadovážiť aj informácie všeobecného i konkrétneho charakteru,
- poplatky za elektronické služby sú nižšie ako za klasické služby.

Výhody elektronického bankovníctva pre banku:

- banka nemusí zamestnávať vyšší počet zamestnancov,
- eliminujú sa zbytočné chyby pri prepisovaní tlačív,
- šetrí sa čas na vybavovanie klientov.

Druhy najviac používaných podvodov v rámci elektronického bankovníctva

Rastúci trend využívania služieb internetového bankovníctva, ako aj slabšia bezpečnostná uvedomelosť a dôverčivosť mnohých používateľov týchto služieb láka rôznych podvodníkov získať citlivé informácie a zneužiť ich vo vlastný prospech. V súčasnosti je internetové bankovníctvo ohrozené nekalým vplyvom hackerov a iných podvodníkov, ktorí sa dopúšťajú trestného činu podvodu podľa § 221 Trestného zákona[8]. Môžeme komunikovať s

---

[6] WAP-banking je ďalšia forma elektronického bankovníctva, ktorá umožňuje klientovi interaktívnu komunikáciu s bankou. Na túto komunikáciu s bankou klient používa mobilný GSM telefón a technológiu WAP. Svojimi možnosťami a spôsobom ovládania pripomína WAP-banking zjednodušený internetbanking.

[7] Homebanking je určený najmä pre tých ľudí, ktorí vykonávajú väčší počet obratov a v rámci toho, že majú záujem zrýchliť komunikáciu s bankou, je pre nich výhodné spracúvanie dát vymieňaných v elektronickej forme. Výhodou je aj to, že týmto spôsobom možno údaje automaticky prenášať do a z účtovníckeho programu či firemného informačného systému.

[8] *§ 221-Podvod*

(1) Kto na škodu cudzieho majetku seba alebo iného obohatí tým, že uvedie niekoho do omylu alebo využije niečí omyl a spôsobí tak na cudzom majetku malú škodu, potrestá sa odňatím slobody až na dva roky.

(2)

Odňatím slobody na jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a spôsobí ním väčšiu škodu.

(3) Odňatím slobody na tri roky až desať rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1

a) a spôsobí ním značnú škodu,

b) z osobitného motívu, alebo

c) závažnejším spôsobom konania.

(4) Odňatím slobody na desať rokov až pätnásť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1

bankovým serverom alebo s podvodníckym serverom, transakcia nie je bezpečná. *„Nové technológie, ako napríklad Internet alebo elektronické bankovníctvo sa menia na extrémne užitočné nástroje na páchanie trestných činov, ako aj na prevod ziskov pochádzajúcich zo zdanlivo legálnych činností. Podvody a korupcia dosahujú obrovské rozmery a útočia na obyvateľov, ako aj na samotné inštitúcie.“*[9]

Podvodníci využívajú viaceré druhy podvodov, známe sú najmä nasledujúce:

Sociálne inžinierstvo

Sociálne inžinierstvo je spôsob získavania citlivých informácií manipuláciou. Zneužíva dôverčivosť ľudí vydávaním sa za zástupcov známych existujúcich spoločností alebo inštitúcií. Metóda bežne využíva telefóny alebo internet.

Phishing

Phishing (odvodené od anglického „fish“ (ryba). Phishing využíva prvky sociálneho inžinierstva. Metóda je charakteristická pokusmi podvodne získať citlivé informácie, ako sú identifikačné a autentifikačné údaje (PID, PIN, kódy z GRID karty) či detaily platobnej karty vydávaním sa za dôveryhodnú osobu alebo spoločnosť. Najčastejšie má podobu falošného oficiálneho e-mailu alebo telefonátu, prostredníctvom ktorého podvodník žiada údaje od používateľa. Vloží odkaz na svoju internetovú stránku, ktorá vyzerá podobne ako stránka banky, od klienta vyžaduje zadať bezpečnostné údaje karty[10]. (Hackeri často v komunikácii používajú namiesto „f“ písmená „ph“.)

Pharming

Pharming – je nasledovník phishingu, kde podvrhnutá stránka využíva malware u klienta tak, že stránka je podobná na stránku banky a nemá viditeľné znaky podvrhu. Pharming je založený na zmene položiek DNS (Domain Name System) napríklad prostredníctvom vírusu alebo modifikovaných súborov ponúknutých na stiahnutie na internete. To znamená, že ak aj používateľ dodržiava jednu zo všeobecných zásad a zadá názov internetovej adresy priamo do adresného riadka internetového prehliadača, internetová stránka, ktorú navštívi, nie je stránka pôvodná, ale falošná. Na rozdiel od phishingu už nemusí kliknúť na odkaz. Po zadaní údajov je presmerovaný na skutočnú banku. Klient prihlásený do internetbankingu si nič nevšimne. Hacker môže v tomto prípade napadnúť priamo aj počítač klienta. Najistejšia je vonkajšia ochrana: autorizačná SMS banky potvrdzujúca každú transakciu.

Trójske kone – skladajú sa z dvoch programov. Jeden je používaný na zabezpečenie prístupu podvodníka priamo k počítaču používaním škodlivého softvéru, ktorý sa nainštaluje a potom otvorí back-door (zadné dvierka), aby mohol hacker vstúpiť. Druhý sa nainštaluje na používateľov počítač v momente, keď je spustený infikovaný súbor. To umožní podvodníkom prístup k hard disku počítača a tým k veľkému objemu osobných informácií o jeho majiteľovi.

Keylogger-malware inštalovaný v počítači klienta, ktorý posiela hackerovi údaje o stlačených klávesoch, z čoho sa dajú zistiť prihlasovacie údaje klienta.

---

a) a spôsobí ním škodu veľkého rozsahu,
b) ako člen nebezpečného zoskupenia, alebo
c) za krízovej situácie

[9] Akčný plán boja proti organizovanému zločinu schváleného Radou Európy dňa 28. apríla 1998, **Jorge ESPINA,** Španielsky prokurátor, predvstupový poradca EÚ pre boj proti korupcii.

[10] Ako sa chrániť? Treba byť opatrný pri sťahovaní programov a používať antivírusový program, ktorý zabráni sledovanie vášho počítača. Adresa internet bankingu začína zabezpečeným https:// namiesto http://.

Spôsoby zneužívania platobných kariet[11]

Množstvo prípadov zneužitia platobnej karty každoročne v SR prudko stúpa, možno konštatovať, že podvody s kartami rastú geometrickým radom. Najčastejším spôsobom zneužitia platobných kariet je ich strata alebo krádež, podvodníci si však dokážu vyrobiť aj falzifikát. Kým po roku 2000 to bolo len niekoľko sto trestných činov neoprávneného vyrobenia a obstarania platobnej karty, minulý rok to bolo už 2347 prípadov. Objasnenosť týchto prípadov sa však pohybuje len na úrovni trinásť percent[12]. Karta sa môže zneužiť viacerými spôsobmi. Buď sa ku karte dostane niekto iný, alebo niekto získa údaje z karty, ktoré sú potrebné na výber peňazí. Polícia má skúsenosti aj s nelegálnym kopírovaním platobných kariet, respektíve s neoprávneným vyrobením, alebo obstaraním platobných kariet a ich zneužitím páchateľmi.[13] Jedným zo spôsobov, ako vyrobiť falošnú platobnú kartu, je odkopírovať údaje z magnetického prúžku na zadnej strane, keď sa jej majiteľ nepozerá. Potom stačí už len odpozorovať identifikačné číslo, pričom preniesť údaje na čistú kartu už nie je problém. Snímač ani čistá karta s magnetickým prúžkom pritom nie sú veľmi drahé záležitosti. Používanie falošných kariet je jednoduchšie pri výbere z bankomatov, pretože pri platení v obchode by ju predajca mohol, vzhľadom na viaceré ochranné prvky rozpoznať.

Táto trestná činnosť súvisiaca so zneužívaním platobných kariet narastá, treba však povedať, že na Slovensku je v obehu viac ako 5 miliónov platobných kariet a k dispozícii je 37 778 bankomatov a terminálov[14].

Pre oprávneného držiteľa platobnej karty[15] je azda najnepríjemnejšou skúsenosťou krádež z účtu na "napichnutom" bankomate. Podvodník tam nainštaluje zariadenie, ktoré nasníma údaje z karty, čím získa prístup k účtu klienta banky. Takto majiteľ karty môže prísť ľahko o všetky úspory.

Najznámejšie spôsoby zneužitia platobných kariet:[16]

- **Phishing a pharming** sú časté spôsoby, ktorých princíp bol objasnený vyššie.
- **Skimming** – odkopírovanie údajov na karte, pomocou ktorých vedia podvodníci vytvoriť falzifikát. Páchatelia sa často spájajú s nepoctivými zamestnancami v baroch, reštauráciách či obchodoch, ktorí prichádzajú často s kartami do styku. Ďalšou formou je získanie údajov prostredníctvom špeciálnych zariadení, ktoré podvodníci inštalujú na kartové sloty na bankomatoch. Páchatelia namontujú do bankomatu skimmovacie (kopírovacie) zariadenie, ktoré načíta údaje o platobnej karte z jej magnetického prúžku. Okrem skimmera ešte páchatelia namontujú minikameru nad klávesnicou na účel nasnímania PIN kódu karty. Kamera je o niečo väčšia ako špendlíková hlavička, takže si ju držitelia kariet ťažko všimnú. Na základe získaných údajov si páchateľ vyrobí falzifikát karty a niekde, väčšinou v zahraničí, vyberie peniaze. Zavedenie čipovej technológie by malo tieto podvody obmedziť. Ako sa chrániť? Skontrolovať, či na otvore na vloženie karty nie je podozrivé zariadenie.
- **Card-trapping** – je jednou z foriem, akú používajú páchatelia na získanie hotovosti pri bankomate. Tento spôsob podvodu sa tiež nazýva **libanonská slučka,** páchateľ do

---

[11] STIERANKA, J., DOBIAŠOVÁ, B. Platobné karty a možnosti ich zneužitia. In *Zborník z 11. medzinárodného sympózia Akadémie Policajného zboru v Bratislave konaného dňa 2. 6. 2010,* s. 45 – 48.

[12] www.aktualne.centrum.sk, 2,6. 2008

[13] http://aktualne.centrum.sk, 2. 6. 2008

[14] Podľa Združenia pre bankové karty SR, stav k 31.12. 2009.

[15] Podľa zákona č. 510/2002 Z. z. § 21, ods. (3) Oprávneným držiteľom elektronického platobného prostriedku (ďalej len "oprávnený držiteľ") je každá fyzická osoba alebo právnická osoba, ktorej vydavateľ vydal na používanie elektronický platobný prostriedok na základe nimi uzavretej zmluvy o vydaní a používaní tohto elektronického platobného prostriedku.

[16] http://financie.etrend.sk/banky 1.2. 2010

otvoru na prijímanie kariet nalepí z vnútornej strany pásku alebo zastrihnutú fóliu a tak zablokuje kartu, ktorá sa nedá vytiahnuť. Toto zariadenie zadrží kartu v jeho slote a „náhodný“ okoloidúci potom klientovi radí, ako znovu skúsiť zadať kód. Páchateľ súri klienta, aby uvoľnil priestor, že si chce vybrať peniaze, môže predstierať, že podobná situácia sa stala aj jemu a majú kontakt na banku, ktorá problém vyrieši. Privolajú domnelého bankového úradníka, ktorý si pýta PIN kód. Keď držiteľ karty naletí a odíde, páchateľ odstráni zariadenie a vyberie peniaze. Ochrana v tomto prípade je jednoduchá, **neopustiť zaseknutú kartu, nenechať si od nikoho radiť, nedávať nikomu PIN kód.**

- **Shoulder surfing** – jednoduchý spôsob, keď podvodníci sledujú zadávanie PIN kódu napríklad do bankomatu „ponad plece“ klienta. Potom sa kartu pokúsia ukradnúť.
- **Card-not-present-fraud** – podvodníci zneužijú neoprávnene získané detailné údaje o kreditnej karte klienta v transakciách, kde karta nie je fyzicky prítomná, napríklad pri obchodoch cez internet či telefón. On-line obchodníci často neverifikujú, či je osoba zadávajúca údaje skutočne vlastníkom karty.[17]
- **Identity theft** – alebo krádež identity, keď podvodníci použijú nelegálne získané osobné doklady napríklad na otvorenie účtu v cudzom mene či získanie kreditnej karty.

Bezpečné používanie elektronického bankovníctva

Odporúčané postupy pri prihlasovaní sa do internetbankingu:[18]

1. Používajte bezpečný internetový prehliadač. Najvhodnejšie sú Firefox, ktorý obsahuje množstvo ochranných prvkov, prípadne Operu, ktorá je málo rozšírená. Používajte kvalitný antivírus aj prostriedky na odhalenie malwaru. Nie je vhodné, aby ste mali zároveň so stránkou internetbankingu otvorenú aj inú internetovú stránku. [19]
2. Vždy **zadávajte internetovú adresu** do adresného riadka internetového prehliadača **ručne. Overte si, či je stránka elektronického bankovníctva, ktorá sa vám otvorila, šifrovaná (začiatok adresy začína https, nie http) a zabezpečená certifikátom.**
3. Nikdy nepristupujte k službe elektronické bankovníctvo z odkazov uvedených v akejkoľvek e-mailovej správe.
4. Používajte heslo, ktoré má mať osem znakov, veľké aj malé písmená, aspoň jeden špeciálny znak (%#-_.? a pod.) a aspoň jednu číslicu. Vyvarujte sa, aby malo toto heslo nejaký zmysel. Čím je dlhšie heslo a prihlasovacie meno, tým lepšie.
5. Najskôr sa prihláste nesprávnym heslom. Ak ste na správnej stránke banky, určite vás odmietne. Ale ak ste na podvrhnutej stránke, nesprávne heslo sa pošle hackerovi a stránka sa vám poďakuje za vloženie hesla a vyhlási nejakú inú chybu. Ak ste si istý, že ste na správnej stránke, prihláste sa druhýkrát svojím skutočným heslom. Ak stránka aj tak zahlási chybu, neváhajte a odpojte počítač od siete. Celkom určite ste sa stali obeťou hackera.
6. Ak prihlasovacia stránka na zadanie prihlasovacích údajov ponúka klávesnicu na obrazovke, použite túto, zabránite tak keyloggeru, aby prečítal vaše prihlasovacie údaje z klávesnice počítača.

---

[17] Podľa zákona č. 510/2002 Z. z. § 21, ods. (10) Oprávnený držiteľ preukazuje svoju totožnosť pri používaní a) bankovej platobnej karty osobným identifikačným číslom alebo podpisom oprávneného držiteľa zhodným s podpisom na bankovej platobnej karte, ak sa vydavateľ s oprávneným držiteľom nedohodne na inej forme preukazovania totožnosti podľa osobitného zákona;

[18] **http://www.zervan.sk/indexN.php?id=84&n=internetove-bankovnictvo-bezpecne, 5.5. 2010, 18.30**

[19] Najčastejšími nositeľmi malware sú stránky s počítačovými hrami a s erotickým obsahom.

7. Ak máte podozrenie, že ste sa stali obeťou hackera, oznámte to čo najskôr svojej banke a zablokujte si účet vrátane platobných kariet. Počítač vypnite a zaneste ho na políciu alebo k špecialistovi, aby zistil, ktorý malware máte nainštalovaný. Niekedy sa dá vystopovať aj hacker, ktorý ho používa. Preto, ak sa niečo také stane, zásadne nečistite počítač, aby ste nezmazali stopy. Hackerstvo je aj u nás trestné.

Odporúčané postupy pri používaní elektronického bankovníctva[20]

- **Neodpovedajte na** e-mailové **správy** a telefonáty **vyzývajúce na uvedenie identifikačných a autentifikačných údajov**, detailov platobnej karty a podobne.
- **Nereagujte na žiadne žiadosti o vyplnenie formulárov na internete** alebo v e-mailovej správe, hlavne ak nabádajú na udanie bankového spojenia a ďalších citlivých informácií.
- **Buďte opatrní pri otváraní príloh e-mailovej správy** hlavne, avšak nielen, **od neznámeho odosielateľa**, keďže môžu obsahovať vírus a iný škodlivý kód.
- **Pri autentifikácii GRID kartou nikdy nezadávajte naraz viac ako jeden kód. Ak stránka nabáda na zadanie viacerých kódov z GRID karty naraz, so stopercentnou istotou ide o podvrhnutú stránku.**
- **Pre bezpečné ukončenie práce s elektronickým bankovníctvom sa odhláste** a zatvorte okno internetového prehliadača.
- **Pri práci s elektronickým bankovníctvom používajte bezpečný počítač, ktorý by mal obsahovať tieto bezpečnostné prvky:**

    - **Legálne nadobudnutý software.**
    - **Automatická aktualizácia operačného systému.**
    - **Antivírusová ochrana.**
    - **Antispyware a antiadware programy** (na zabránenie nepovoleného zbierania informácií z počítača, sledovania internetových činností a zvyklostí používateľa). **Osobný firewall (**slúži na zabezpečenie kontroly toku dát medzi počítačom a internetom).
    - **Aktualizácia programov, ktoré pristupujú na internet**, a to hlavne internetový prehliadač, ale aj komunikačné programy (ICQ, Skype a pod.).

Literatúra

KUMMER, R , TALLO, A. Kriminalita v oblasti moderní telekomunikační techniky I. In *Policajná teória a prax, roč. XV., č. 3, 2007, s. 73 – 81.*

STIERANKA, J., DOBIAŠOVÁ, B. Platobné karty a možnosti ich zneužitia. In *Zborník z 11. medzinárodného sympózia Akadémie Policajného zboru v Bratislave konaného dňa 2. 6. 2010*, s. 45 – 48.

TUREČEK, J. et. al. *Policejní technika.* Vydavatelství a nakladatelství Aleš Čeněk, Plzeň 2008, s. 198 -210. ISBN 978-80-7380-119-9.

Trestný zákon č. 300/2005 Z. z. , § 221, v znení neskorších predpisov.

Zákon č. 510/2002 Z. z. § 21, ods. (10) o platobnom styku a o zmene a doplnení niektorých zákonov.

http://www.zervan.sk/indexN.php?id=84&n=internetove-bankovnictvo-bezpecne, 5.5. 2010, 18.30

[20] https://ibs.luba/sk.ebweb/do/start, 5.5.2010, 17.30 hod.

https://ibs.luba/sk.ebweb/do/start, 5. 5. 2010, 17.30 hod.
http://aktualne.centrum.sk , 2. 6. 2008
http://financie.etrend.sk/banky 1. 2. 2010

Keywords: electronic banking, internet banking, credit cards, Phishing, Pharming, Trojan horses, skimming, card-trapping, "fraud.

Summary

Using information and communication technology is growing worldwide at tremendous pace. Society is now entirely dependent on ICT[21], and is naturally exposed to attacks conducted in this area. Given the above, it is understandable that the area of electronic banking, which uses modern communication technology on a large scale is at risk of being affected.

Banks combine known elements to ensure access to clients' accounts through the Internet in various ways, from free combinations with maximum convenience to overcombined with many security features – from PIN to the smart card logon. Forms of electronic banking - Telephone banking (Phonebanking)[22] - GSM - banking (SMS) - internetbanking - E-mailbanking, wap-banking, home banking, credit cards and more.

Electronic Banking brings a number of advantages to the client and to the bank. The benefits of electronic banking for clients include: the opportunity to work with those in the comfort of office, at home, but also on the move not only in Slovakia but also in other countries, wherever possible access to telephone and Internet, electronic banking is available 24 hours a day , 7 days a week, offering time savings and more. The benefits of electronic banking for the bank: bank may employ a larger number of well-paid employees, eliminate unnecessary forms, a clerical errors, saving the time dealing with clients.

The growing trend of using online banking and trust of many users of these services attract different fraudsters to obtain sensitive information and to use it in their own favor. Today, internet banking is at risk of not genuine influence of hackers and other fraudsters committing the crime of fraud under § 221 of the Criminal Code. Fraudsters use various types of fraud, while the following are most common: social engineering, Phishing, Pharming Trojan horses, keyloggers - malware, skimming, card-trapping, Shoudersurfing, Card-Not-Present-Fraud, Identity Theft.

Best tips when using electronic banking:
• Make sure the e-banking site that you open is encrypted (start address begins with https, not http) and secured by certificate. Security is created by SSL security protocol.
• Use a password that has eight characters, upper and lower case letters, at least one special character (%#-_.? etc..) and at least one digit. Avoid this password to have any meaning.
• Entering changes (proactive approach) is a possible after typing an SMS key or by using an electronic signature stored on a smart card.
• Is it possible to enter limited financial transactions.

[21] ICT - Information and Communication Technologies
[22] Two forms of phonebankingu: Interactive Voice Responcer (IVR) - a machine that can communicate with the client by voice and carries out orders given by them, Call Center - mediated communication via telephone operator who conducts operations with the support of banking information system, similar to interaction with an employee at the counter. Some banks include the use of faxes (for example faxing through an account statements) in the phonebanking.

• Do not respond to e-mail messages and phone calls asking for an identification and authentication data, details of payment cards and the like.
• Do not respond to any request to fill in forms on the Internet.
• Be careful when opening attachments to the e-mail message, especially as they may contain viruses and other malicious code.
• When authentification by a GRID card, never enter more than one code at once.
• For the safe completion of work with electronic banking log off and close the browser.
• When working with electronic banking, always use safe computer.

Ing. Beata Dobiašová
Československá obchodná banka
e-mail: bdobiasova@csob.sk

Recenzent: doc. Ing. Jan Váňa, CSc.