Počítačová kriminalita v bankovnictví

Computer crime in banking

Jiří Šohaj

Bakalářská práce
2008

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2007/2008

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jiří ŠOHAJ**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Počítačová kriminalita v bankovnictví**

Zásady pro vypracování:

1. **Práci zpracujte jako edukační materiál do předmětu Kriminalistické technologie a systémy.**
2. **Vyjmenujte a rozeberte příklady možných útoků na elektronické bankovnictví.**
3. **Zaměřte se na další typy počítačové kriminality v bankovnictví.**
4. **Navrhněte možnou obranu ze strany klienta banky.**
5. **Analyzujte možné druhy ochrany před neoprávněným přístupem do aplikace elektronického bankovnictví.**
6. **Uveďte způsoby ochrany majitelů platebních karet před jejich zneužitím.**
7. **Materiál opatřete tabulkou a obrazovou dokumentací.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **James, Lance. Phishing bez záhad. Praha : Grada Publishing, a.s., 2007. ISBN 978-80-247-1766-1.**
2. **Matějka, Michal. Počítačová kriminalita. Prah : Computer Press, 2002. ISBN 80-7226-419-2.**
3. **Endorf, Carl, Schultz, Eugene a Mellander, Jim. Hacking - detekce a prevence počítačového útoku. Praha : Grada Publishing, a.s., 2005. ISBN 80-247-1035-8.**
4. **Pavel Satrapa. Phishing - nový trend v podvodných dopisech - LUPA. LUPA. [Online] Internet Info, s.r.o., 20. 05 2004. http://www.lupa.cz/clanky/phishing-novy-trend-v-podvodnych-dopisech/.**
5. **Ondřej Bitto. Rhybaření střídá pharming - LUPA. LUPA. [Online] Internet Info, s.r.o., 31. 03 2005. http://www.lupa.cz/clanky/rhybareni-strida-pharming/.**
6. **Marie Faturová. Podvodů s kopírováním bankovních karet přibývá - iDNES.cz. iDNES.cz. [Online] MAFRA a.s., 24. 10 2007. http://ekonomika.idnes.cz/podvodu-s-kopirovanim-bankovnich-karet-pribyva-f5x-/ekonomika.asp?c=A071024_121835_ekonomika_maf.**

Vedoucí bakalářské práce: **JUDr. Vladislav Štefka**
Ústav elektrotechniky a měření

Datum zadání bakalářské práce: **22. února 2008**

Termín odevzdání bakalářské práce: **3. června 2008**

Ve Zlíně dne 22. února 2008

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

V bakalářské práci se zabývám zejména nebezpečím, které číhá na uživatele výpočetní techniky při komunikaci se svou bankou, ale nejen s ní. V první části mé práce pohlížím na počítačovou kriminalitu v době jejího počátku u nás i ve světě. Po krátkém ohlédnutí následuje zhodnocení stavu, ve kterém se počítačová kriminalita v bankovnictví nachází nyní. V této části objasňuji hlavní druhy kybernetického zločinu. Zajímavou kapitolou práce jsou rady všem uživatelům bankomatů, které jsou shrnuty do několika přehledných bodů.

V druhé části se zabývám nedávnými útoky na klienty České spořitelny. Zde můžeme vidět praktické ukázky podvodných e-mailů, jejichž prostřednictvím se útočníci snažili na klientech zmíněné banky vymámit jejich citlivá osobní data, a následně také jejich rozbor.

Cílem mé práce je předat čtenářům cenné informace, které jim do budoucna mohou být velmi nápomocné.

Klíčová slova: phishing, pharming, skimming, spoofing.

ABSTRACT

I deal about the particular danger which waiting for users of computer technology in communication with their bank in my bachelor thesis. I regard computer criminality at the time its beginning in the Czech Republic and abroad in first part of my work. After short looking back follows estimation state in which the computer criminality in banking finds now.

In those parts bring out main sorts cybernetic crime. Interesting part of my work is counsel to all users of cash dispenser that are lumped to the several well - arranged points.

I deal with late attacks on clients of Česká spořitelna in second part.

Here we can see practical exhibits of fraud e-mails, whose through attackers try on clients mentioned banks cadge their sensitive personal data, and subsequently also their analysis.

Aim of my work is hand over reader's valuable information, which can be very helpful for them.

Keywords: phishing, pharming, skimming, spoofing.

Nad vypracováním této práce měl odborný dohled a neocenitelnými radami vedl mé myšlenky JUDr. Vladislav Štefka, kterému bych za jeho projevenou ochotu a spolupráci na tomto místě rád poděkoval.

Prohlašuji, že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně ……

Podpis diplomanta

OBSAH

ÚVOD

Počítačová kriminalita (cyber-crime, kyberzločin) je rozsáhlým pojmem a nelze ho jednoznačně definovat. "Počítačová kriminalita" je určité slovní spojení, jímž se označuje skupina trestných činů mající stejný charakter, stejně jako je tomu u pojmů např. hospodářská kriminalita, násilná kriminalita, apod. Z diskusí především let devadesátých nakonec vyplynul názor, „že počítačovou kriminalitu je třeba chápat jako páchání trestné činnosti, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat) nebo pouze některá z jeho komponent, případné větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti“[1] (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti. Definice počítačové kriminality, která je akceptována v rámci Evropské unie je taková, že počítačová kriminalita je nemorální a neoprávněné jednání, které zahrnuje zneužití údajů získaných prostřednictvím informačních a komunikačních technologií nebo jejich změnu. Často se pojem počítačová kriminalita používá i pro tradiční formy kriminality, u níž byly počítače nebo počítačové sítě použity, aby ji usnadnily. Určujícím operacionálním elementem je přitom vždy způsob zneužití výpočetní techniky, vzhledem k jejím specifickým vlastnostem a dominantnímu postavení mezi věcnými komponentami způsobu páchání konkrétního trestného činu. Jelikož je tato problematika velmi obšírná a zasahuje do rozmanitých částí kriminální trestné činnosti, nemůže proto existovat jednotný způsob boje proti ní. Jednotlivé trestné činy proto šetří a objasňují policisté zařazení na příslušných odděleních, která je mají v popisu své každodenní pracovní náplně. Například fiktivní převody nebo krádeže peněz řeší hospodářská kriminálka stejně jako počítačové pirátství, které je útokem na duševní vlastnictví. Pornografie však spadá do působnosti mravnostního oddělení.

V bankovním sektoru se můžeme setkat s různými druhy počítačové kriminality, které budu v této práci dále podrobně rozebírat.

[1] Smejkal Vladimír: Internet @ §§§. Praha. Grada Publishing, spol. s r.o.. 1999.

I. TEORETICKÁ ČÁST

1 HISTORIE

1.1 Ve světě

Za první „počítačový" zločin je v literatuře považován případ, který se udál ve Francii v roce 1801, tedy téměř 150 let před vznikem prvního skutečného počítače. Tkadlec Jacquard tehdy sestrojil jednoduché zařízení, které dovolovalo automatizovat a opakovaně provádět jednotlivé úkony používané při tkaní speciálních látek. Zaměstnanci Jacquardovy manufaktury byli z tohoto „vynálezu" natolik konsternováni, že ve strachu před ztrátou pracovních míst donutili za pomocí série sabotáží pana Jacquarda od dalšího vývoje jeho strojku upustit. Později, respektive v 70. letech devatenáctého století, bylo možné zaznamenat z dnešního pohledu celkem nevinné žertíky náctiletých chlapců, kteří obsluhovali telefonní ústředny. Dlouhý čas služby si mnohdy krátili spojováním k sobě nepatřících hovorů, jejich jakoby náhodným přerušováním nebo chichotáním do telefonu. Poté, co se začaly množit stížnosti na podobné jednání, byli chlapci v roli telefonistů v roce 1878 nahrazeni pečlivějšími a odpovědnějšími dívkami a se žertíky byl konec, a to na dost dlouhou dobu. Spojení počítače a telefonní linky a jeho využití k tvorbě rozsáhlých počítačových sítí přijde až za dalších 100 let.

1.2 V České republice

Až do konce 80. let nebylo vůbec možné o počítačové kriminalitě v ČSSR mluvit, neboť téměř neexistovala domácnost, která by měla osobní počítač. Informační technologie patřily k embargovanému zboží pro dovoz do zemí socialistického tábora, tudíž každý dovoz byl vlastně již od počátku nelegální. Výpočetní technika vesměs původem ze Sovětského svazu, kterou provozovalo několik podniků a univerzit, sestrojovaná v provizorních podmínkách a neustále kontrolovaná podezřívavým komunistickým režimem, zajisté neskýtala příliš mnoho možností pro počítačové piráty.

Situace se změnila koncem 80. let, kdy k nám byly (vesměs podloudně, například pracovníky tehdejší Československé plavby labsko-oderské na lodích z německého Hamburku) dovezeny první počítače, například značek Sinclair, Atari či Commodore. K tomu se přidružila ještě česká výroba počítačů Didaktik, IQ či PMD. Zakrátko začal čile fungovat „trh" s hrami a aplikacemi pro tyto počítače. Vznikla nezapomenutelná éra, v níž kralovaly především počítače Sinclair ZX Spectrum, případně některé modely Atari.

Jistě mnoho dnešních počítačových odborníků prodělalo svou první zkušenost s informačními technologiemi nad hrami typu Flappy, Boulder Dash, Manic Miner či Pacman, nahrávaných do skrovné paměti počítače nekonečně dlouhou dobu z magnetofonových kazet, s neustálou hrozbou přerušení nahrávání a nutností začínat znovu. O legálnosti takto šířeného SW nemohla být vůbec řeč, koneckonců šlo jednak o embargované technologie, ale ani česká legislativa z oblasti autorského práva s existencí počítačů nepočítala. K nelegálním šiřitelům software patřil i stát, který napomáhal k šíření počítačových programů pomocí kroužků počítačové techniky organizovaných například v rámci organizace SVAZARM, městských a okresních Stanic mladých techniků, škol apod.

První počítačový zločin, který literatura uvádí, je datován ještě ze 70. let a jeho skutečná existence je neověřená. Mělo se jednat o poškození záznamových pásek magnetem spáchané pracovníkem Úřadu důchodového zabezpečení. Oficiální informace o rozsudku však neexistují (případ měl být kvalifikován jako sabotáž). Doklad existuje o případu poškození počítače sovětské výroby SMEP z roku 1987. „Programátoři chtěli cíleným poškozování počítače dosáhnout jeho výměny za kvalitnější přístroj západní výroby. Případ byl tehdejší justicí kvalifikován jako sabotáž, později překvalifikován na mírnější poškozování socialistického majetku a nakonec bylo z důvodu amnestie trestní stíhání zcela zastaveno.“[2]

„Nikterak ojedinělé nebyly ani machinace s výpočetní technikou v mzdových účtárnách, či jiných pracovištích umožňujících manipulaci s penězi. Jen v 80. letech bylo zaznamenáno 14 takových deliktů. Byly vesměs kvalifikovány jako rozkrádání majetku v socialistickém vlastnictví.“[3]

Další skupinou počítačových trestných činů bylo zneužívání počítačů zaměstnavatele k soukromým aktivitám, ať už zábavním, nebo za účelem obohacení, podle tehdejší právní úpravy trestný čin neoprávněného užívání majetku v socialistickém vlastnictví. „Jeden z prvních případů tohoto typu se udál v 80. letech na brněnském Vysokém učení technickém, kdy si zaměstnanec počítačového centra pro své vlastní potřeby na počítačích zaměstnavatele zpracovával agendu bytových družstev. Pracovník byl souzen, ale stíhání

[2] Matějka Michal: Počítačová kriminalita. Praha. Computer Press. 2002.
[3] Matějka Michal: Počítačová kriminalita. Praha. Computer Press. 2002.

přerušila amnestie. Obhajoba tehdy vycházela z toho, že tato práce nebyla na úkor zaměstnavatele, a že tedy nikdo nebyl poškozen.“[4]

Zajímavou událostí na území tehdejší už České a Slovenské Federativní Republiky bylo oficiální připojení země k Internetu. Stalo se tak 13. 2. 1992, zpočátku ovšem bez jakéhokoliv nabízení přístupu mimo akademickou síť.

Policie se od počátku snažila nelegálnímu šíření software zabránit. Počátkem devadesátých let ovšem byla obeznámenost s touto problematikou velmi nízká, a to jak v řadách obyvatelstva, tak v řadách orgánů činných v trestním řízení. Podle statistik dosahovala u nás míra používání nelegálního software tehdy až 80 % (oproti 39 %[5] v roce 2007). „Situace se začala zvolna měnit, jednak docházelo k růstu kupní síly obyvatelstva, dále osvěta přinesla větší podvědomí o problému nelegálního software.“[6]

[4] Matějka Michal: Počítačová kriminalita. Praha. Computer Press. 2002.
[5] Dostupný z WWW: http://www.bsa.cz
[6] Matějka Michal: Počítačová kriminalita. Praha. Computer Press. 2002.

2 SOUČASNOST

V současné době je škála trestných činů páchaných pomocí počítače velmi široká. Z toho důvodu se budeme věnovat pouze trestným činům, které jsou páchány v bankovním sektoru.

2.1 Phishing

2.1.1 Co to je?

Slovo phishing vzniklo z anglického password fishing (volně přeloženo znamená rybaření hesel). Náhrada prvního f za stejně znějící ph má několik vysvětlení. Nejpravděpodobnější je přirovnání k tzv. phreakingu, resp. obecně je záměna f za ph běžná v tzv. LeetSpeak, slangu používaném v jisté internetové subkultuře (takzvaných Internet scammers). V češtině se slovo používá velmi často neupravené, případně se používá „počeštěná" varianta rhybaření, případně rhybhaření, rhybolov, rhybholov, toto je však poněkud umělé, anglická homofonie ph-f v češtině protějšek nemá. Někde se můžeme setkat i s teorií o vzniku tohoto slova, která tvrdí že je složeno ze tří slov password harvesting fishing, tzn. „rybolov sklízením hesel". Ta je však chybná. Souhrnně označuje phishing různé podvržené a zfalšované e-maily, webové stránky apod., které se z Vás pokoušejí dostat důvěrné informace. Respektive ne přímo podvodné e-maily (stránky), ale jejich odesílatelé (majitelé), kteří je potom zneužívají. Podle serveru antiphising.org se jim to daří poměrně dobře. Útokům takovýchto podvodníků totiž podle tohoto serveru podléhá kolem 5% procent oslovených. Což na nenáročnost a průhlednost triku je opravdu dost. Další nepříznivou zprávou je, že počet těchto útoků neustále roste.

Phishing existuje již 13 let, začalo to s America Online (AOL) v roce 1995. Objevily se programy, které automatizovaly proces phishingu v souvislosti s údaji o účtu a platebních kartách. Tehdy se phishing v oblasti elektronické pošty nepoužíval tolik jako u Internet Relay Chat (IRC - chatování po internetu) nebo systému upozorňování na nové zprávy používaného u America Online. Podvodníci napodobovali administrátora od America Online, sdělovali obětem, že se objevil problém s vyúčtováním a že je třeba obnovit údaje o platební kartě a přihlašovací údaje. „Tehdy byla tato metoda vcelku úspěšná, protože

spojení domácího osobního počítače a připojení k internetu bylo prakticky novinkou. Nezasahovala však takovou část populace jako dnešní phishing.“[7]

Náhlý útok phishingu proti finančním institucím byl poprvé zaznamenán v červenci 2003. Terčem byly hlavně E-LOAN, e-gold, Wells Fargo a Citibank.

1	PayPal	3980
2	Bank of America Corporation	3750
3	eBay, Inc.	2508
4	HSBC Group	1181
5	NatWest Bank	223
6	Poste Italiane	152
7	HSBC	105
8	Wells Fargo	104
9	JPMorgan Chase and Co.	86
10	Banca di Roma	77

Tabulka 1 - nejvíce napadané společnosti v dubnu 2008

[zdroj: www.phishtank.com]

Nejpozoruhodnější fintou fenoménu phishingu bylo, že přinesl novou kategorii typů útoku, na kterou se nedostávalo v rozpočtu na zabezpečení informačních technologií u téměř všech finančních institucí: lidský faktor. Všechny ty nákladné firewally, certifikáty SSL (Secure Sockets Layer), pravidla šifrované komunikace s bankou a bezpečnostní management nemohly zastavit zneužívání důvěry v on-line operace. „Tento fenomén nejen že zkompromitoval důvěrné uživatelské údaje, ale měl dokonce zásadní dopad na důvěru klientů ohledně telekomunikace mezi institucí a jejími klienty.“[8]

Prvním případem pokusu o uplatnění phishingu v prostředí bankovní sféry České republiky se v březnu 2006 stala Citibank.

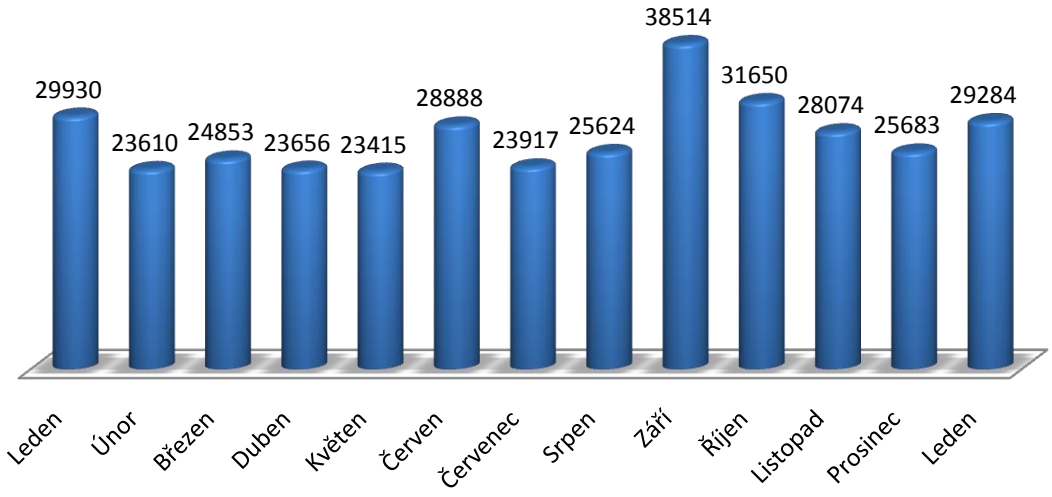
Znalost PIN umožní útočníkům využít kartu, jako kdyby ji měli. Znalost CCV (poslední tři čísla z kódu uvedeného na zadní straně karty) jim umožní kartu využít pro online nákupy. Zda o všechny peníze přijdete, či nikoliv, záleží na smluvních podmínkách dané banky a také na dalších bezpečnostních opatřeních. Nikde není zaručeno, že z Vašeho účtu bude

[7] Lance James: Phishing bez záhad. Praha. Grada Publishing. 2007.
[8] Lance James: Phishing bez záhad. Praha. Grada Publishing. 2007.

čerpáno bezprostředně poté, co jste nevědomě poskytli své osobní údaje. Může se to stát dny až týdny poté a Vy si zpravidla už ani nevzpomenete, co jste kdy udělali špatně.

V případě podvodných e-mailů snažících se vylákat osobní data klientů, kdy jedna hromadná zásilka čítá 100 000 e-mailů, může být úspěšnost až 5% kliknutí na odkaz (5000 možných obětí). Ne všichni, ale svá data poskytnou. Mnoho lidí zadá úmyslně nepravdivé nebo neúplné informace. Každá hromadná zásilka tedy může nasbírat 10 až 100 obětí. Míra návratnosti se pohybuje mezi 0,01 a 0,1%. Ale lidé, kteří padnou za oběť téměř vždy, sdělí vše, na co se phisheři ptají: jména, adresy, účty, čísla platebních karet a mnoho dalších osobních údajů.

„Znalost údajů pro přístup k online bankovnictví může být stejně nebezpečná. Je potřeba si uvědomit, že řada online bankovních služeb není nijak dodatečně zabezpečena – opravdu někdy stačí zadat údaje a uskutečnit převod peněz. Vystopovat majitele případného účtu, kam byly přesunuty Vaše peníze, se pak může změnit ve stejnou hru na kočku a myš jako hledání útočníků.“[9] Je důležité, aby internetové bankovnictví mělo dodatečné bezpečnostní prvky - například použití čipové karty s certifikátem, bez které nejde nic udělat, nebo schvalování transakcí se zapojením mobilního telefonu.



Graf 1 - počet phishingových útoků za období leden 2007 - leden 2008
[zdroj: www.antiphishing.org]

[9] Dostupný na WWW: http://www.lupa.cz

2.1.2 Jak poznat, že jde o podvod?

Dalo by se říct, že phishing je takovým bratříčkem hoaxu (poplašných zpráv), má i některé jeho znaky. Na příkladech si ukážeme, jak na první pohled poznat, že jde o phishing.

Dobrý den uživateli služby xxx,

chtěli bychom Vás upozornit, že dochází k inovaci naší databáze, čímž by mělo dojít k výraznému zlepšení služeb. Z naší nabídky namátkou vybíráme:

- nabídka nových služeb

- lepší ochrana proti odhalení Vašeho hesla

- atd.

Z výše vypsaného důvodu Vás tedy žádáme, abyste na adrese: http://neco.cz vyplnil znovu Vaše přihlašovací údaje (neposílejte svoje údaje jako odpověď na tento mail), které se uloží přímo do již připravené nové databáze. Pokud informace nevložíte, nejsme bohužel schopni na Vaší registraci brát zřetel a Vy budete muset projít celou registrační fází znovu. Předem děkujeme za Vaši ochotu a těšíme se na další společnou spolupráci.

Váš Admin služby xxx

Takto nějak by mohl vypadat e-mail, který dostane adresát do schránky, pak už útočník pouze čeká na to, jak se zachová. Samozřejmě v podobném duchu se nese i odkaz, kde se většinou nachází formulář na vyplnění údajů, pro věrohodnost takové stránky je provázaná s originální stránkou poskytovatele služby (banka, hosting, atd.). K tomu se ještě dostaneme. Z pomyslného druhého soudku je e-mail(web) s takovýmto obsahem:

Vážený zákazníku,

domníváme se, že se na našem serveru nacházejí tzv. mrtvá konta, což jsou konta, která byla za poslední tři měsíce neaktivní, a proto nepředpokládáme, že se některý uživatel k takovému kontu ještě vrátí. Abychom si byli 100% jistí, prosím vyplňte údaje na následující stránce: xxx.yyyy.zz. Děkujeme za spolupráci a doufáme, že nám zachováte přízeň. Pokud nemáte s naší službou nic společného, hluboce se omlouváme a tento e-mail ignorujte.

Další, zcela odlišný typ zprávy, je pokus o přemluvení uživatele, aby si změnil heslo sám, e-mail by mohl vypadat takto:

Vážený uživateli,

z důvodu opravy (inovace, ...), která bude provedena mezi dny dd.mm.rrrr - dd.mm.rrrr bychom Vás chtěli požádat o změnu hesla na heslo námi vygenerované: h83BS73fm (nějaký neskutečný řetězec znaků a čísel). Neučiníte-li tak, můžete přijít o svoje data.

Váš admin

Takových vzorových e-mailů existují stovky. Nebudeme si je tady všechny uvádět, ale raději se podíváme na jejich společné znaky. Jsou to:

chyby - gramatické, slohové, překlepy… - bohudík, část takovýchto podvodníků svoje útoky uspěchává, proto se v nich často objevují do očí bijící chyby. Je sice pravda, že takový nepovedený dopis může napsat i sekretářka, ale ona je za to placená, má určité vzdělání a její sloh by měl být na jisté úrovni.

neformálnost - tento znak souvisí tak trochu s prvním. Je to opět způsobeno tím, že někteří autoři (amatéři) si nepotrpí na formálnost a tak můžou používat nespisovné a neformální výrazy. Což by se u profesionální firmy nemělo stávat.

hodně technických výrazů - docela používaná metoda je také zamotání hlavy uživatele. Útočník využívá neznalosti většiny uživatelů a celou zprávu zabalí do cizích a odborných slov, kterým třeba ani sám nerozumí. Vlastně to není ani potřeba. Účelem je zmást uživatele, což se většinou podaří a procento úspěšnosti útočníka se tím pádem zvyšuje.

zprávy bez diakritiky – snad každý, kdo používá internet ke komunikaci, určitě ví, že většina lidí píše bez diakritiky, a to z důvodu rozdílného nastavení kódování různých uživatelů, podpory jednotlivých národních znaků v různých aplikacích apod. Ale nezasvěcený člověk (sekretářka, která by normálně dostala napsání oznámení na starost) toto určitě neudělá. Takže když se objeví ve schránce email nebo odkaz na stránky bez diakritiky, je to určitě podvod. Podobně pokud útočník rozesílá své maily pomocí PHP (Hypertext Preprocessor, původně: Personal Home Page - jedná se o skriptovací programovací jazyk, který je určen především pro programování dynamických internetových stránek), bude pravděpodobně používat také text psaný bez diakritiky,

protože narazí na problém s kódováním češtiny. Samozřejmě některým nastavením hlavičky mailu jde toto odstranit, ale to je věc jiná.

vykřičníky - dalším varováním může být, když se na konci věty objeví dva a více vykřičníků, otazníků nebo teček. Takováto přehnaná interpunkce se používá hlavně u hoaxů a jelikož je phishing hoaxům velmi podobný, může se vyskytovat i zde.

modré z nebe, metoda cukru a biče - další věc je slibování různých bonusů a výhod buď v nové (fiktivní) verzi služby anebo přímo za vyplnění choulostivých údajů (vyplňte jméno a heslo a uvidíte Britney Spears nahou) anebo naopak různých hrozeb, nevyplníte-li to, co se po Vás žádá.

nátlak, panika - útočník se může pokoušet vyvinout nátlak, donutit adresáta panikařit, aby nemohl racionálně přemýšlet a vyplnil to, co žádá. Obvykle se straší ztrátou dat nebo zrušení celého účtu, ale samozřejmě to může být úplně něco jiného, v kreativitě se meze nekladou.

nearogantní chování - ačkoli se může útočník pokusit o nátlak, bude vždy 100% slušný. Žádné arogantní chování čekat rozhodně nemůžete. Nakonec, je to útočník, který žádá službu, ne Vy. I když u soukromých subjektů by slušnost k zákazníkovi měla být též na předním místě, nezřídka se s arogantním nebo povýšeným chováním můžeme zejména ze strany poskytovatelů služeb zdarma setkat.

neodpovídat přímo na mail - jako poslední znak jsem vybral, že v každém podvodném e-mailu by nemělo chybět prohlášení ve smyslu, že na emailovou adresu, ze které přišel e-mail, v žádném případě neodpovídejte, a to proto, že 99,99% procent takových e-mailů je zfalšovaných. Ale na to ještě dojde. I když by byl kontakt od skutečného poskytovatele, je 100% jistota, že uvede mail na případné dotazy, telefonní číslo a jméno osoby, kterou je třeba kontaktovat. Útočník to neudělá.

2.1.3 Technická stránka

Veškeré přemlouvání by bylo k ničemu, kdyby útočník založil např.: bezplatný účet ve tvaru banka.freehosting.nictonestoji.cz a žádal tam zadání přihlašovacích údajů k homebankingu například České spořitelny. Proto se rhybholovníci pokouší udělat vše proto, abyste se domnívali, že se skutečně nacházíte na správné stránce. Některé hojně používané technické metody si představíme.

2.1.3.1 Zfalšování hlavičky mailu

Snad každý rhybholovník umí zfalšovat hlavičku e-mailu tak, aby běžný uživatel nepoznal, že políčko "od:" není pravdivé. Jednak na internetu najdete množství nástrojů na poslání takového e-mailu, jednak se to dá nastavit pomocí PHP.

Obrana: Stačí si pozorně přečíst hlavičku e-mailu, hlavně dejte pozor na pole "odesílatel:", kde byste měli nalézt informace o všech smtp[10] serverech a tak se dovíte, odkud mail skutečně pochází. Horší je, když útočník odesílá mail pomocí smtp serveru, ze kterého Vám může přijít mail i od skutečného poskytovatele (například přijde mail od administrator@seznam.cz přes smtp seznamu s phishingovým obsahem). Naštěstí takovéto servery většinou vkládají do hlavičky IP adresu (jednoznačná identifikace konkrétního zařízení) člověka, který daný mail odesílá. Bohužel hlubší rozbor hlavičky je pro běžného uživatele složitý.

2.1.3.2 Podobnost

V tomto případě útočník využívá nepozornosti uživatelů. Například si zaregistruje doménu hodně podobnou doméně nějaké instituce či služby a za ni se pak vydává. V praxi to pak vypadá tak, že například stránka www.k-banka.cz je kopie stránky www.kb.cz s tím rozdílem, že ji nespravuje Komerční banka, ale nějaký rhybolovník, který Vám právě krade peníze z účtu. Nejhorší na tom je, že si toho nemusíte všimnout hned, protože stránka může odkazovat na stránku pravou, a tak například po zadání přihlašovacích údajů se můžete ocitnout na stránce pravé a se svým účtem normálně pracovat.

Obrana: v tomto případě pomůže být pozorný a pečlivě si všechno ověřovat. Na takovou stránku se dostanete pravděpodobně z odkazu v e-mailu. Teď jsou minimálně dvě možnosti:

a) mail informuje o nové doméně - v tomto případě je dobré prověřit doménu databází whois (např. http://www.whois-search.com nebo http://www.dnsstuff.com), podívat se na starou doménu. Kdyby se přecházelo na jinou, bude tam o tom určitě zpráva nebo přímo kontakt na helpdesk (zákaznickou podporu).

---

[10] Simple Mail Transfer Protocol – internetový protokol určený pro přenos zpráv elektronické pošty (e-mailů) mezi stanicemi.

b) neinformuje - v tomto případě si zkontrolujte, jestli daná adresa souhlasí přesně s adresou, kterou normálně k přístupu na službu používáte. Pozor na záměny (www.paypa1.com není www.paypal.com [jednička místo písmene el], a podobně.)

2.1.3.3 IDN

Je to zkratka slova International Domain Name a znamená, že v doménovém jméně se mohou objevovat také národní znaky (kdyby to měla cz doména, mohli byste mít URL[11] třeba http://www.háčkyčárky.cz), což je na jednu stranu zajímavé, ale horší je, že tento systém je nedokonalý z hlediska převádění znaků na ASCII[12] hodnoty a tak dvě různé domény může browser (prohlížeč) vyhodnotit jako jednu a tu samou, což je pro rhybholovníky jako dělané.

Obrana: jediné řešení, na které tvůrci browseru přišli, je pouze vypnutí podpory IDN, což sice není ideální, ale ochrání Vás. Pokud přece jen chcete mít IDN zapnuté, musíte pečlivě kontrolovat cíl, kam odkaz vede.

2.1.3.4 Přihlašování se z jiných stránek

Další věc, kterou se můžete nechat lehce zlákat a dokonce ani nemusíte poznat, že jde o podvod, jsou nabídky přihlásit se ke svému účtu z jiné stránky. Autor stránek se může tvářit, jako že Vám prokazuje službu, že zbytečně nemusíte přecházet na další stránku, protože se můžete přihlásit přímo přes něj ke své oblíbené službě. Dokonce to i povětšinou funguje tak jak má, akorát že autor mimochodem ukládá někam do souboru nebo databáze všechny hesla a uživatelská jména, které jeho stránkou projdou.

2.1.3.5 Chyby

Jak jsem již zmiňoval (chyba v IDN), oblíbené chyby jsou *adres* nebo *status bar spoofingy*, to je když v adres baru (tam kde píšete adresu stránky) nebo v status baru (lišta dole s informacemi) se objevují jiné URL adresy než na jaké skutečně klikáte (právě případ IDN) nebo vložení jiných URL do špatně napsaných skriptů. Například www.domena.tld/script.cgi?redirect=www.jinadomena.tld. Na tuto chybu byl nedávno

---

[11] URL - Uniform Resource Locator - definuje doménovou adresu serveru, umístění zdroje na serveru a protokol, kterým je možné zdroj zpřístupnit.
[12] ASCII - Kódová tabulka, která definuje znaky anglické abecedy a jiné znaky používané v informatice.

náchylný obchodní dům e-bay. Toto vložení může být také ve formě vyskakovacích oken. Pamatujte: do vyskakovacích oken důvěrné informace nikdy nevyplňujte, téměř vždy se jedná o podvod.

Obrázek 1 – maskovaná adresa [zdroj: www.microsoft.cz]

Obrana: Sledovat bezpečnostní servery, které o chybách prohlížečů informují a aktualizovat, i když občas (zvlášť v případě IE) se aktualizace dostavují poněkud pozdě.

2.1.4 Rekapitulace phishingu

Jak ho poznáme

- Snaží se vzbudit dojem, že byl odeslán organizací, z jejíchž klientů se snaží vylákat důvěrné informace. Toho se snaží docílit grafickou podobou e-mailu a zfalšováním adresy odesílatele.
- Text může vypadat jako informace o neprovedení platby, výzva k aktualizaci bezpečnostních údajů, oznámení o dočasném zablokování účtu či platební karty, průzkum klientské spokojenosti nebo jako elektronický bulletin pro klienty.
- V textu zprávy je odkaz, který na první pohled většinou vypadá, že směřuje na stránky organizace (banky). Při jeho bližším prozkoumání zjistíte, že ve skutečnosti odkazuje na jiné místo, kde jsou umístěny podvodné stránky (tzv. spoofing).

Jak poznáme podvodné stránky

- Formulář vybízí k vyplnění důvěrných informací, které by banka neměla požadovat.
- V adresním řádku prohlížeče se zobrazuje adresa, která nepatří organizaci, jejichž stránky se snaží napodobit. Uvedená adresa se může snažit originální stránky napodobit, ale vždy bude jiná, případně může začínat číselným kódem IP adresy. Vyskytují se i případy, kdy se podvodníci snaží tuto skutečnost maskovat.
- Ve většině případů podvodů komunikace probíhá po běžném, nezabezpečeném protokolu (adresa začíná http:// a ne https://).

Jak se bránit

- Na odkazy v e-mailu neklikejte. Přesměrují Vás na podvodné stránky, které se Vás mohou snažit oklamat a pokusit se vylákat důvěryhodné informace, ale také mohou obsahovat škodlivé kódy, které se Vám pokusí instalovat do počítače.
- Jestliže potřebujete vstoupit na stránky internetového bankovnictví nebo na stránky příslušné organizace, raději napište internetovou adresu do prohlížeče sami.
- Dejte pozor na překlepy. Podvodníci si mohou dočasně zaregistrovat adresu, která se bude pouze nepatrnou změnou písmen lišit od pravé. Při překlepu se nepozorný uživatel může dostat na falešné stránky.
- Pokud se Vaše elektronické bankovnictví chová nestandardně nebo jsou po Vás požadovány jiné údaje než obvykle, nezadávejte je. Ukončete svoji činnost a kontaktujte zákaznické centrum banky. Existuje další trik podvodníků, tzv. pharming (v další kapitole si ho podrobněji rozebereme). Ten umožňuje přesměrovat uživatele na podvodné stránky, aniž by si toho všimnul, a to i za předpokladu, že dodrží oba předchozí body.
- Používejte aktualizovaný operační systém. V aktualizacích bývají opraveny objevené bezpečnostní chyby, které jinak mohou být zneužity. Většina systémů umí, při správném nastavení, kontrolovat aktualizace sama.
- Používejte antivirový program. Aktualizujte ho. Existují kvalitní antivirové programy, které jsou pro domácí použití zdarma, případně si můžete zakoupit i komerční produkty. Pokud je počítač připojený k Internetu, dokáže si antivirový program (při správném nastavení) stáhnout aktualizaci sám. Neaktualizovaný antivir nemusí včas odhalit nové viry.
- Používejte antispywarové programy, využívejte firewall. Antispywarové programy dokáží odhalit další druhy škodlivého software. O jejich aktualizaci platí totéž, co v předchozích případech. Firewall chrání před nežádoucím přístupem zvenčí nebo může zabránit odchozímu spojení pochybných programů do Internetu.
- Nespouštějte neznámé programy, které Vám přijdou e-mailem, ani na které e-mail odkazuje. Dodržujte nejvyšší opatrnost, přestože zpráva může vypadat, že je od Vašich nejbližších přátel. Typickým příkladem z poslední doby jsou různé podvržené odkazy na elektronické pohlednice. Ve skutečnosti se nekalé živly snaží z odkazované stránky nainstalovat do počítače škodlivý program. Také programy, které se Vám na různých

stránkách snaží vnutit, mohou mnohdy škodit. Například kromě popisované funkčnosti mohou obsahovat i trojské koně, které pracují ve prospěch svých tvůrců.

- K elektronickému bankovnictví nebo ke svým účtům (nejen bankovním) se nepřihlašujte z veřejně přístupných nebo nedůvěryhodných počítačů, které nemáte pod kontrolou. Mohou být na nich nainstalovány různé programy pro monitorování činnosti a Vaše důvěrné informace nebo přístupové kódy se mohou dostat k neoprávněným osobám. Toto se týká nejen počítačů v internetových kavárnách, ale také třeba u známých, kde jsou instalovány programy z různých zdrojů a nemáte jistotu jejich zabezpečení.
- Jestliže nemůžete mít pro svoji práci svůj počítač, který nesdílíte s ostatními členy rodiny, mějte každý svůj účet. Uživatelům nepřidělujte práva administrátora. Získáte tím částečnou ochranu před nežádoucími úpravami systému.
- Používejte svůj rozum a zdravý úsudek. Pamatujte, že útočníci jsou vždy o krok napřed a stále zkoušejí nové triky, jak Vás nachytat. I přes veškeré technologické zabezpečení se může objevit jednoduchý trik, kterým se Vás mohou snažit obelstít. Jestliže nebudete dodržovat základní bezpečnostní pravidla a nepřemýšlet nad svojí činností, můžete se stát další obětí.

2.1.5 Budoucnost

Budoucnost pro nás, běžné uživatele elektronických služeb, bohužel nevypadá dobře. Tuto práci píšu hlavně v důsledku toho, že se o phishingu začalo mluvit jako o vážné hrozbě a že počet útoků neustále roste. Dokonce se na začátku roku začalo mluvit o tom, že letošní rok bude právě rokem phishingu (berte s rezervou). Problém je v tom, že hodně lidí je náchylných a útočník snadno dostane, jak se říká, za málo peněz hodně muziky.

2.2 Pharming

Pharming je bratrem phishingu, mladším, sofistikovanějším a především nebezpečnějším. Ke své činnosti využívá překladu jména serveru na odpovídající IP adresu (každý počítač v síti má svoji jedinečnou adresu, která vypadá například takto: 123.321.88.33.), útočí tedy na DNS (Domain Name System)[13]. Pokud pak uživatel ve svém internetovém prohlížeči zadá adresu například www.vasbankovnidum.cz, nedojde k překladu na odpovídající IP adresu 192.168.1.88, nýbrž nějakou jinou, podvrženou k nerozeznání podobnou a zde je kámen úrazu. Jelikož by pro běžné uživatele počítačových sítí bylo velice obtížné pamatovat si číselné adresy, existuje systém specializovaných počítačů, které převádějí zapamatovatelná doménová jména, tedy např. www.vasbankovnidum.cz, na číselné IP adresy a opačně. Pokud by se totiž útočníkovi podařilo změnit DNS záznam výše zmiňované imaginární banky www.vasbankovnidum.cz, přesměruje se komunikace na jiný stroj, jiné stránky, které však na první pohled nelze rozpoznat od originálu. Nic netušící uživatel tedy zadá požadované přihlašovací údaje a bez větších překážek jimi obdaruje útočníka.

2.2.1 Technická stránka

Jak se přesměrování na falešnou stránku děje? Existují v podstatě dvě možnosti. Pokud je útok zaměřen globálně, napadne útočník tzv. DNS server, na kterém je uložena databáze internetových domén a příslušných IP adres, a tento záznam pozmění. V tomto případě všichni uživatelé, kteří používají daný DNS server, jsou při zadání domény internetového bankovnictví přesměrování na server útočníka.

Tak daleko však v případě současných útoků zřejmě nejsme, protože úroveň zabezpečení DNS serverů bývá relativně vysoká. Pokud Vám celý postup nápadně připomíná techniku DNS spoofingu, máte pravdu. Pharming lze s trochou "štěstí" provést také lokálně modifikací souboru hosts - tzv. "lokální" pharming. Zmiňovaný soubor hosts můžete pod operačním systémem Windows nalézt v adresáři C:\%WINDIR%\system32\drivers\etc, kde %WINDIR% je instalační adresář Windows. Hosts může obsahovat například údaje

[13] DNS je hierarchický systém doménových jmen. Hlavním úkolem jsou vzájemné převody doménových jmen a IP adres.

jako na obrázku 2, kde v prvním sloupci jsou uvedeny IP adresy odpovídající názvům vpravo.

Obrázek 2 – soubor hosts [zdroj: vlastní]

Pokud uživatel zadá ve svém webovém prohlížeči URL www.vasbankovnidum.cz, pak bude přesně podle údaje v souboru hosts kontaktován stroj s adresou 192.168.1.88.

Pharming spočívající v modifikaci souboru hosts by pak mohl vypadat takto:

1. Útočník si vytvoří na první pohled identickou kopii stránek www.vasbankovnidum.cz, díky které bude po nic netušícím uživateli požadovat zadání citlivých údajů o jeho osobě.
2. Tyto podvodné stránky umístí například na stroj s IP adresou 192.168.1.88.
3. Přidá do souboru hosts na vybraném počítači řádek

   192.168.1.88 www.vasbankovnidum.cz
4. Čeká, až se oběť přihlásí ke svému účtu na adrese www.vasbankovnidum.cz .

„Přístup do souboru hosts na vzdáleném počítači může útočník získat například použitím trojského koně, kterého předtím uživateli podstrčil.“[14]

[14] Dostupný z WWW: http://www.lupa.cz

2.2.2 Obrana

Samotné přepsání údajů zajišťují různé počítačové viry, např. trojští koně, kteří se do počítače uživatele dostanou např. v e-mailech nebo v softwaru, který si instaluje, nebo z internetu. Soubor hosts je možné i uzamknout, to ale může způsobovat problémy při běhu některých síťových aplikací. Z toho plyne, že jedinou a nejúčinnější obranou proti tomuto způsobu útoku je použití kvalitního antivirového systému a jeho pravidelná aktualizace. Cestu za úspěchem útočníkovi dále může ztížit správně nakonfigurovaný firewall, nicméně obrana proti pharmingu není v globále vůbec jednoduchá.

2.3 Skimming

Skimming je podvodný postup, při kterém dochází k překopírování originálních údajů z elektronického proužku karty na jinou kartu. Tato data pak je možné použít při platbě bez přítomnosti karty nebo výrobě padělku.

2.3.1 Kde se s ním setkáme

Nejčastěji ke skimmingu dochází zejména v barech, restauracích, někdy na čerpacích stanicích nebo i v hotelech. Pracovník, který chce provést skimming, k tomu používá různé triky, výmluvy nebo manipulační nátlaky na držitele karty. Snaží se o odvedení pozornosti klienta, aby mohl údaje zkopírovat, a někdy provede skimming i za cenu neuskutečnění prodeje zboží nebo služby, aby nevzbudil podezření dvojí manipulací kartou. Pracovník může během platby kartou použít miniaturní kopírovací zařízení a zkopírovat elektronická data z magnetického proužku. Tato data pak mohou být použita buď při platbách bez přítomnosti karty, nebo k výrobě padělané karty. K těmto transakcím pak dochází bez vědomí držitele karty. Podvodníci je ale instalují i na bankomaty. Tento typ podvodu se masivně rozrůstá.

Podvodníci instalují kopírovací zařízení zejména v Praze a středních Čechách. V hlavním městě vzrostl počet z 9 případů v roce 2006 na 28 případů v roce 2007. Ve Středočeském kraji ze dvou na dvanáct. Ostatní kraje zpravidla tak postiženy nejsou.

2.3.2 Technická stránka

Skimmovací zařízení se skládá ze dvou částí. Jedna načítá data vložené platební karty a druhá umožňuje získat PIN[15]. Pokud je zařízení nainstalováno v bankomatu, není na první pohled nic patrné. Snímací prvek je připevněn na šachtu, do které se vkládá platební karta, PIN pak podvodníci získávají pomocí miniaturní kamery (fotoaparátu), která je umístěna v malé vyvrtané dírce v liště u klávesnice. Do lišty je vyvrtána nepatrná dírka, kterou kamera či fotoaparát snímá číslo PIN. Tento způsob kopírování karet ustupuje do pozadí. Podvodníci totiž našli nový, který může být v budoucnu mnohem nebezpečnější. Místo miniaturního kopírovacího zařízení a průhledné falešné klávesnice nyní nasazují podvodníci na bankomaty celý falešný ovládací panel.

Obrázek 3 – skimmovací nástavec [zdroj: www.zive.sk]

Tento panel je navíc od toho originálního téměř k nerozeznání. Případy nového způsobu kopírování karet se už několik měsíců objevují v zahraničí. Nyní však novinka dorazila i k nám. Dosud se nejvíce falešných ovládacích panelů bankomatů objevilo v Praze. Zatímco v roce 2006 bylo dle statistik Policie České republiky zaznamenáno 15 případů, do září 2007 už jejich počet narostl na více než 54. Množství případů je však pravděpodobně mnohem větší.

[15] PIN – Personal Identification Number, což znamená osobní identifikační číslo. Jedná se o jedinečný identifikátor, pomocí kterého je možné se autorizovat např. platební karty, mobilní telefony, vstupní kódy apod.

2.3.3 Obrana

Banky začínají výrazně zvyšovat bezpečnost svých bankomatů pomocí tzv. FDI (Fraudulent Device Inhibitor) bezpečnostního modulu. Tento modul výrazně omezuje skimming karet, tedy kopírování informací na platební kartě. FDI moduly dosud fungují jen v několika zemích světa. Instalací modulu na bankomaty se dle bankovních domů úplně zamezilo skimmingu karet. Podle odborníků tomu tak není, protože podvodníci jsou vždy o krok napřed a je jen otázkou času, kdy začnou používat skimmovací nástavce na tyto bezpečnostní prvky.

V současné době se tyto moduly používají například na Novém Zélandě, ve Francii, Španělsku či Německu. Další státy jako Singapur, Hong Kong či Kanada začínají moduly instalovat.

Obrázek 4 – kamera v držáku na letáky snímá zadávání PINu

[zdroj: www.zive.sk]

Kromě nového bezpečnostního zařízení banky spouští i nový vzhled obrazovky bankomatu. Obrazovka klienta upozorňuje právě na nový bezpečnostní prvek, aby bylo zabráněno nejistotě klientů, než se povědomí o zařízení dostatečně rozšíří.

2.3.4 Budoucnost

Snad definitivní konec skimmingu se dostaví za několik let, až všechny banky přejdou z karet s magnetickým proužkem na čipové. Bankám se do přechodu na čipové karty moc nechce. Je pro ně výhodnější nahradit klientovi škodu, než investovat do technologií. Do té doby nezbývá nic jiného než maximální obezřetnost. Zakrývejte si proto svůj prostor při zadávání PINu, nevkládejte kartu do bankomatu v případě, že to jde ztěžka či trhaně. A pokud pojmete jakékoliv podezření, informujte o něm policii nebo dotyčnou banku.[16]

Obrázek 5 – FDI bezpečnostní modul
[zdroj: www.cibc.com]

[16] Dostupný na WWW: http://podnikani.centrum.cz

Desatero správného chování u bankomatu

1. Před použitím bankomatu zkontrolujte, zda nenese stopy neoprávněného zásahu. Pokud Vám karta nejde snadno zasunout do štěrbiny nebo se kolem bankomatu pohybují podezřelí lidé, nepoužívejte jej a vyhledejte raději jiný bankomat.
2. Pokud se domníváte, že do bankomatu někdo neoprávněně zasáhl, sdělte tuto skutečnost policii, vydavateli karty nebo provozovateli bankomatu. Svou pozorností chráníte nejen sebe, ale i ostatní držitele karet.
3. Při čekání dodržujte diskrétní zónu a umožněte vybírajícímu provést nerušeně celou transakci. U některých bankomatů je doporučená diskrétní zóna vyznačena na zemi.
4. Stůjte těsně u bankomatu a při zadávání PINu zakrývejte klávesnici volnou rukou shora a tělem zamezte případnému odpozorování PINu přes rameno.
5. Nikomu nedovolte, aby odvedl vaši pozornost. Pokud se na vás někdo mačká nebo sleduje, zrušte transakci pomocí tlačítka "storno" nebo "zrušit (cancel)", vyčkejte potvrzení o zrušení transakce a přejděte k jinému bankomatu.
6. Při výběru hotovosti z bankomatu se vždy řiďte výhradně pokyny na obrazovce. Nepřijímejte pomoc od neznámé "dobré duše", nikdy se nenechte vyrušit a odvést svou pozornost od transakce.
7. Nikdo kromě Vás nemá oprávnění Vaši operaci přerušit před dokončením (ani pracovníci banky, obsluha bankomatu, pracovník bezpečnostní služby či policie, atd.)
8. Nikdy neopouštějte bankomat před dokončením celé transakce. Po dokončení transakce si nezapomeňte odebrat hotovost a Vaši kartu. Ještě před opuštěním bankomatu si oboje diskrétně uložte.
9. Pokud se na obrazovce bankomatu nezobrazí oznámení o zadržení karty, nepředpokládejte, že se Vaše banka automaticky dozví, že bankomat kartu zadržel.
10. Pokud jste začali používat bankomat a karta Vám bez vysvětlení nebyla vrácena, od bankomatu raději neodcházejte a ihned kontaktujte vydavatele karty, který Vám pomůže s dalším postupem.[17]

[17] Dostupný z WWW: http://fincentrum.idnes.cz

2.4 Pojmy použité v textu

Jelikož se v předešlých kapitolách o phishingu i pharmingu objevovaly pojmy, které nemusí být pro každého známé, rád bych Vás s nimi blíže seznámil.

2.4.1 Spoofing

Technika, při které se určitý uzel sítě vydává za někoho jiného - proto, aby místo něj přijímal věci, ke kterým by jinak neměl mít přístup nebo aby jeho jménem naopak vysílal něco, co by sám vysílat buď nemohl, nebo alespoň ne s požadovaným efektem. Takovéto techniky, pro které se vžilo označení spoofing (doslova: napálit, převézt, vodit za nos), patří mezi nejnebezpečnější zbraně těch, kteří chtějí neoprávněně proniknout do cizích sítí. Naštěstí ale i proti technikám „spoofingu" dnes existují dostatečně účinné protizbraně a ochranná opatření.

Ne vždy je ale „spoofing" věcí zavrženíhodnou. Někdy je naopak praktikován zcela záměrně, protože přináší pozitivní efekt nebo dokonce zachraňuje situaci, která by jinak byla neudržitelná. Vysvětlení tkví v chování mnoha současných síťových protokolů, které byly vyvinuty pro prostředí lokálních počítačových sítí. Tyto protokoly si pravidelně „osahávají" celou síť jako takovou i její jednotlivé uzly a posílají jim dotazy typu „jsi ještě naživu?". Důvodem pro tuto činnost je snaha průběžně detekovat případné změny v topologii sítě, v dostupnosti jednotlivých uzlů či další relevantní události, a adekvátně na ně reagovat dříve, než způsobí nějaké problémy. Příkladem může být snaha serveru udržovat si přehled o existenci a funkceschopnosti jednotlivých stanic v roli klientů - co když třeba nějaký uživatel vypne svůj počítač, aniž se odhlásil od serveru? Při explicitním odhlášení totiž server může uvolnit všechny zdroje, které pro uživatele na dané stanici vyhradil. Pokud je ale uživatelův počítač vypnut bez odhlášení, nedozvěděl by se o této možnosti a příslušné zdroje by musel rezervovat i nadále.

V lokálních sítích, které obvykle mají relativně velkou přenosovou kapacitu (alespoň ve srovnání se sítěmi rozlehlými), je režie na pravidelné „osahávání" vcelku zanedbatelná a techniky založené na tomto principu jsou zde používány dosti často. Frekvence, s jakou se „osahávání" opakuje, může samozřejmě být různá, ale obvykle se pohybuje od desítek sekund po jednotky minut.

Problém ale vzniká v případě, kdy do hry vstoupí sítě rozlehlé, například jako forma propojení dvou od sebe poněkud vzdálených lokálních sítí. Pravidelné „osahávání" zde

může odčerpávat již poměrně významnou část přenosové kapacity, protože ta bývá v rozlehlých sítích často mnohem menší. Ještě větší nebezpečí však může číhat v samotné pravidelnosti nejrůznějšího „osahávání".

Lokální sítě mají totiž ještě jednu zajímavou odlišnost od sítí rozlehlých - fungují většinou na nespojovaném principu, zatímco sítě rozlehlé fungují nejčastěji na principu spojovaném. V praxi to znamená, že v lokálních sítích se jednotlivé bloky dat (pakety) odesílají bez předchozího navázání spojení s příjemcem, zatímco v rozlehlých sítích se při spojovaném přenosu spojení s příjemcem navazuje. Kromě toho se v rozlehlých sítích mnohdy (zvláště jde-li o tzv. veřejné datové sítě) platí za objem přenesených dat a většinou také za dobu existence spojení. Přitom se ale praktikují různé techniky směřující k optimalizaci nákladů uživatele i celkové propustnosti sítě - například to, že když po stanovený čas nejsou v rámci určitého spojení přenášena žádná data, je toto spojení automaticky zrušeno (a v případě nového požadavku na přenos zase znovu navázáno). „Ekonomický efekt samozřejmě závisí na konkrétních podmínkách, ale může být opravdu významný - pokud ale není celý úsporný mechanismus znehodnocen pravidelným „osahováním". Zde pak přichází k dobru výše citovaný „spoofing", díky kterému nemusí být propouštěna „osahávací" data do pomalejší rozlehlé sítě, a předem určené a pověřené zařízení, nacházející se ještě v dané lokální síti, generuje falešné odpovědi simulující kladnou odpověď vzdáleného uzlu. Má to samozřejmě i svá úskalí - co když skutečné zařízení přestane být dosažitelné, nebo alespoň nějak jinak změní svůj stav? Díky spoofingu se toto nepozná."[18]

2.4.2 Trojský kůň

Trojský kůň je uživateli skrytá část programu nebo aplikace s funkcí, se kterou uživatel nesouhlasí (typicky je to činnost škodlivá). Název trojský kůň pochází z antického příběhu o dobytí Tróje.

Trojský kůň může být samostatný program, který se tváří užitečně – například hra, spořič obrazovky nebo nějaký jednoduchý nástroj. Časté jsou spořiče obrazovky s erotikou nebo pornografií. Někdy se trojský kůň vydává za program k odstraňování malware[19] (dokonce

[18] NaMíček internetový magazín č. 1/2006.
[19] Počítačový program určený ke vniknutí nebo poškození počítačového systému.

jako takový může fungovat a odstraňovat konkurenční malware). Tato funkčnost slouží ale pouze jako maskování záškodnické činnosti, kterou v sobě trojský kůň ukrývá.

V Microsoft Windows může trojský kůň využít toho, že řada programů včetně systémového správce souborů (exploreru) skrývá přípony souborů. Vypadá pak jako soubor s obrázkem, zvukem, archivem nebo čímkoliv jiným, přestože se ve skutečnosti jedná o spustitelný kód. Chce-li uživatel obrázek kliknutím zobrazit, je ve skutečnosti spuštěn program (trojský kůň).

Trojský kůň může být ale také přidán do stávající aplikace. Poté je upravená verze šířena například pomocí peer-to-peer sítí (doslova rovný s rovným) neboli P2P. Je to tedy označení architektury počítačových sítí, ve které spolu komunikují přímo jednotliví klienti (uživatelé) nebo warez servery (termín počítačového slangu označující autorská díla, se kterými je nakládáno v rozporu s autorským právem). Uživatel stažením kopie aplikace, nejčastěji bez platné licence nebo jako volně šířený program z nedůvěryhodného serveru, může získat pozměněnou kopii aplikace obsahující část programového kódu trojského koně dodaného třetí stranou.

2.5 Padělání bankovek a cenných papírů

Peníze se padělají od doby, kdy se začaly jako platidlo používat. Svědčí o tom archeologické nálezy padělatelských dílen zařízených na ražbu mincí i drakonické tresty, které měly už v dávných dobách od této činnosti každého odradit. Dnes sice odhalený padělatel nepropadne hrdlem, ale i tak může počítat s mnohaletým vězením. Souboj mezi národními bankami emitujícími platidla a padělateli rozhodně neztrácí na intenzitě, jen se s technickým pokrokem přesouvá na stále vyšší úroveň.

Šance, že narazíte na padělek, není velká, ale rozhodně to není vyloučeno. Podle České národní banky připadá na jeden milion bankovek v oběhu přes třicet zjištěných padělků, u eurobankovek pak skoro dvakrát více. Největší nebezpečí na Vás číhá tam, kde se bankovkám při placení nevěnuje velká pozornost, platí se v nepřehledné situaci, špatným osvětlení, typickým třeba v různých hernách a barech, při pouličním prodeji atd. Věnovat pozornost bankovkám, které Vám někdo vrací při placení, se však vyplatí všude.

Padělky bankovek se hodnotí podle pětibodové stupnice:

- 5 - neumělý padělek - kvalita je opravdu bídná a padělek lehce rozeznatelný
- 4 - méně zdařilý padělek
- 3 - zdařilý padělek
- 2 - nebezpečný padělek
- 1 - velmi nebezpečný padělek - téměř se neliší od originálu

Odhalit padělky zařazené do prvních dvou stupňů (5 - neumělý padělek a 4 - méně zdařilý padělek) by nemělo činit potíže nikomu, kdo je gramotný a všímavý. Tyto padělky, kterých je zatím nejvíce, se od originálu výrazně liší barevným provedením, kvalitou tisku i papíru. Ochranné prvky na nich buď zcela chybějí nebo jsou jen velmi nedokonale napodobeny.

V poslední době však přibývá i padělků, které už laik rozpoznat nemusí. Díky dostupnosti velmi kvalitní kopírovací a tiskové techniky včetně speciálního grafického softwaru se stále častěji objevují padělky třetího a druhého stupně (zdařilé a nebezpečné). Výskyt padělků prvního stupně (velmi nebezpečný padělek) je naštěstí poměrně řídký. Vyrobit takto kvalitní padělek, který od originálu rozezná pouze školený odborník, vyžaduje padělatelskou dílnu se zcela speciálním vybavením a zkušeným personálem.

Ochranné prvky na bankovkách

1. Vodoznak
2. Ochranný okénkový proužek
3. Ochranná vlákna
4. Soutisková značka
5. Skrytý obrazec
6. Opticky proměnlivá barva
7. Iridiscentní pruh
8. Mikrotext

Obrázek 6 – ochranné prvky na bankovce – líc

[zdroj: www.cnb.cz]

Obrázek 7 – ochranné prvky na bankovce – rub

[zdroj: www.cnb.cz]

II. PRAKTICKÁ ČÁST

3 PHISHING

3.1 Útok na Českou spořitelnu

Od počátku roku 2008 začaly masivní útoky na klienty České spořitelny, které se až do Velikonoc stupňovaly. Nejdříve to byly úsměvné pokusy s neumělou češtinou. S největší pravděpodobností se jednalo o strojové překlady a oslovení "Drahoušek zákazník" se stalo oblíbeným sloganem. Další pokusy varovaly před neprovedenou transakcí nebo slibovaly odměnu za vyplnění dotazníku. Všechny tyto podvodné e-maily byly psány buď anglicky nebo nepovedenou češtinou. Zlom nastal až ve chvíli, kdy podvodníci použili velmi jednoduchý trik. Text jednoduše okopírovali přímo ze stránek České spořitelny. Zneužili aktualitu, která varuje před podvodnými e-maily. V textu sice varovali před sebou samými, ale nechyběl odkaz na "verifikaci" svého účtu, který samozřejmě směřoval na podvodné stránky.

Proto si příklady ukážeme právě na těchto útocích. Jde o desítky různých e-mailů spojených s desítkami různých verzí webů.

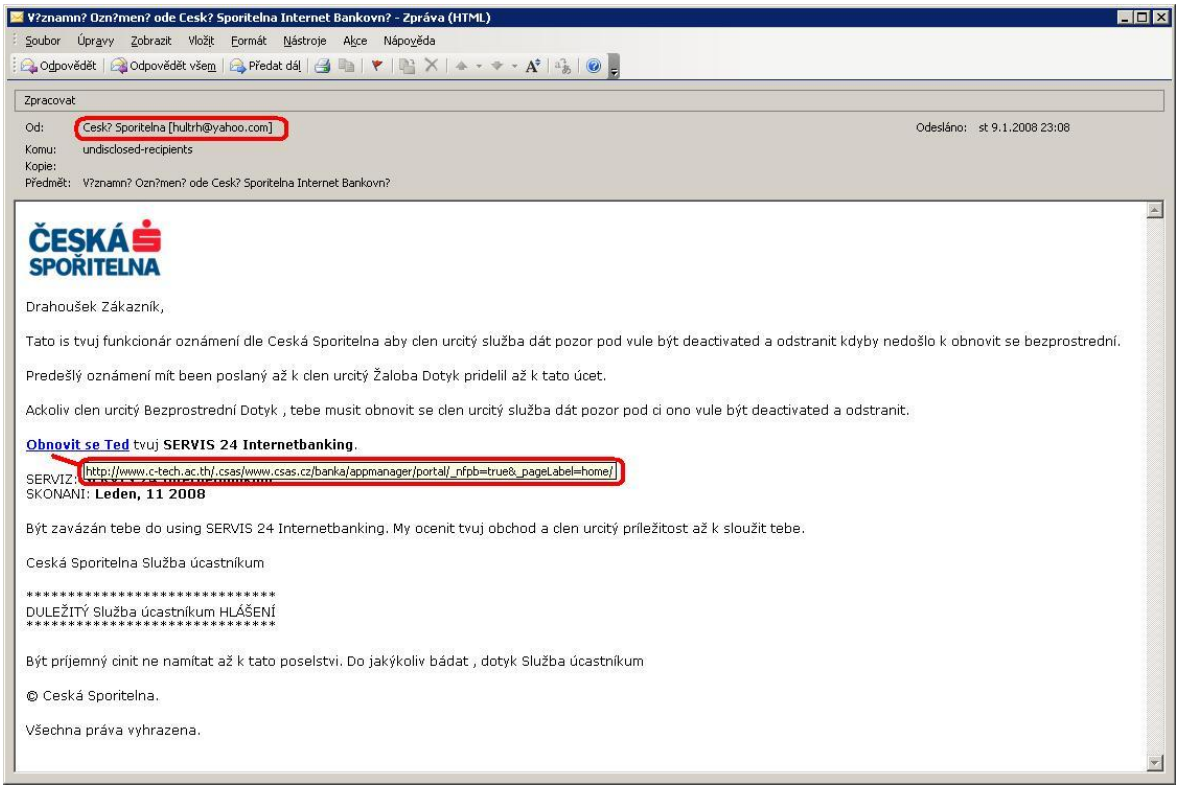
Ty střídají využití přihlášení do internetového bankovnictví, ověření údajů platební karty z nějakého pro klienta významného důvodu i skvělou možnost získat 1500 až 2500 korun jako odměnu za vyplnění dotazníků o spokojenosti se službami.

Zatímco webové stránky jsou zpravidla perfektní kopií skutečných stránek České spořitelny (až na několik exemplářů, kde došlo ke ztrátě některých českých znaků), e-maily jsou na tom hůře. Většina z nich je výplodem automatického překladače, přesto se najdou perfektně zpracované e-maily, na kterých je vidět, že se na jejich tvorbě musel podílet někdo, kdo zná češtinu. Ne všechny e-maily je totiž možné získat z nějakého vzoru, který by Česká spořitelna používala.

Útok na Českou spořitelnu bych rozdělil do několika vln, které se lišily svým zpracováním.

3.1.1 1. vlna

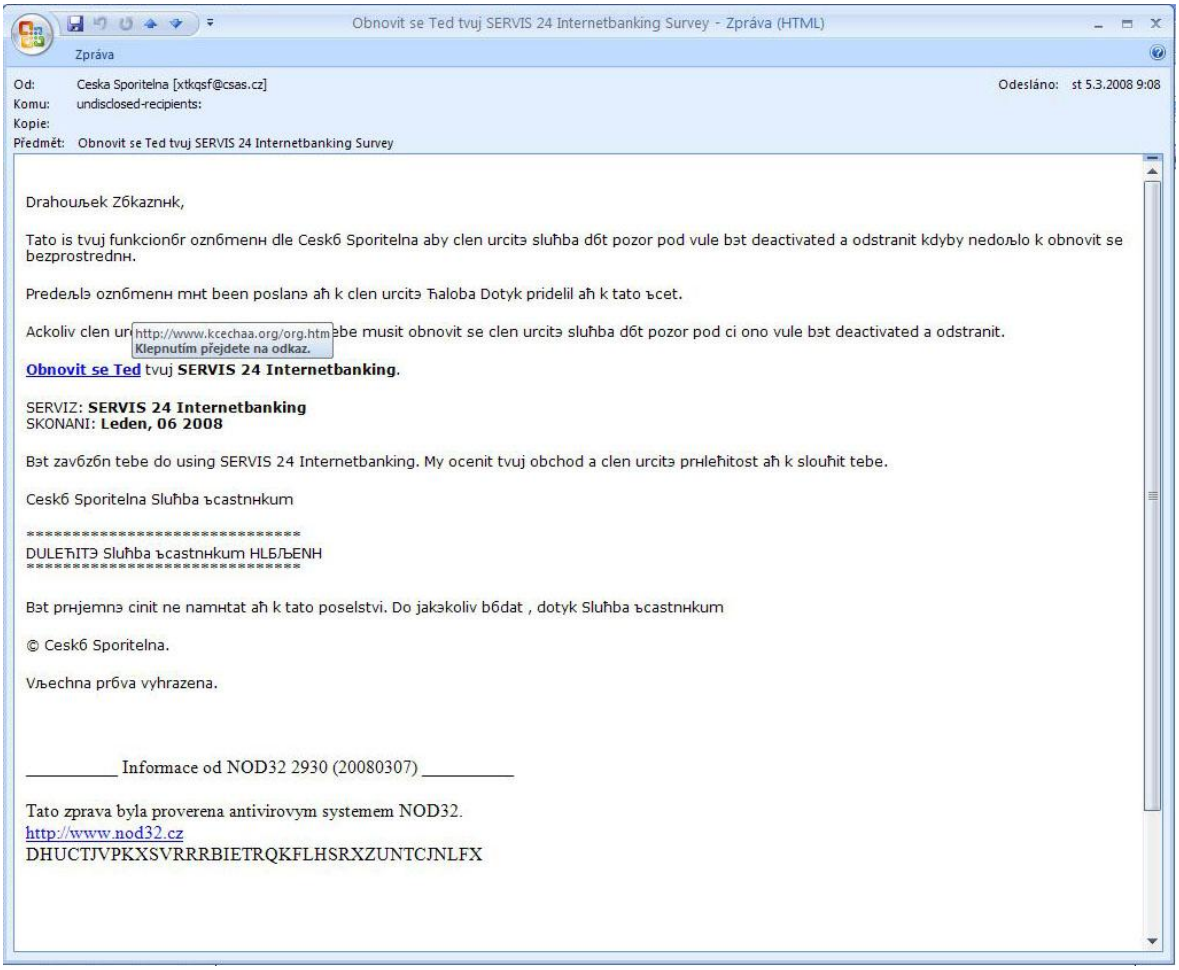
E-maily byly psány lámanou češtinou, bylo vidět, že byl použitý překladač.



Obrázek 8 – email z první vlny [zdroj: www.phishing.cz]

3.1.2 2. vlna

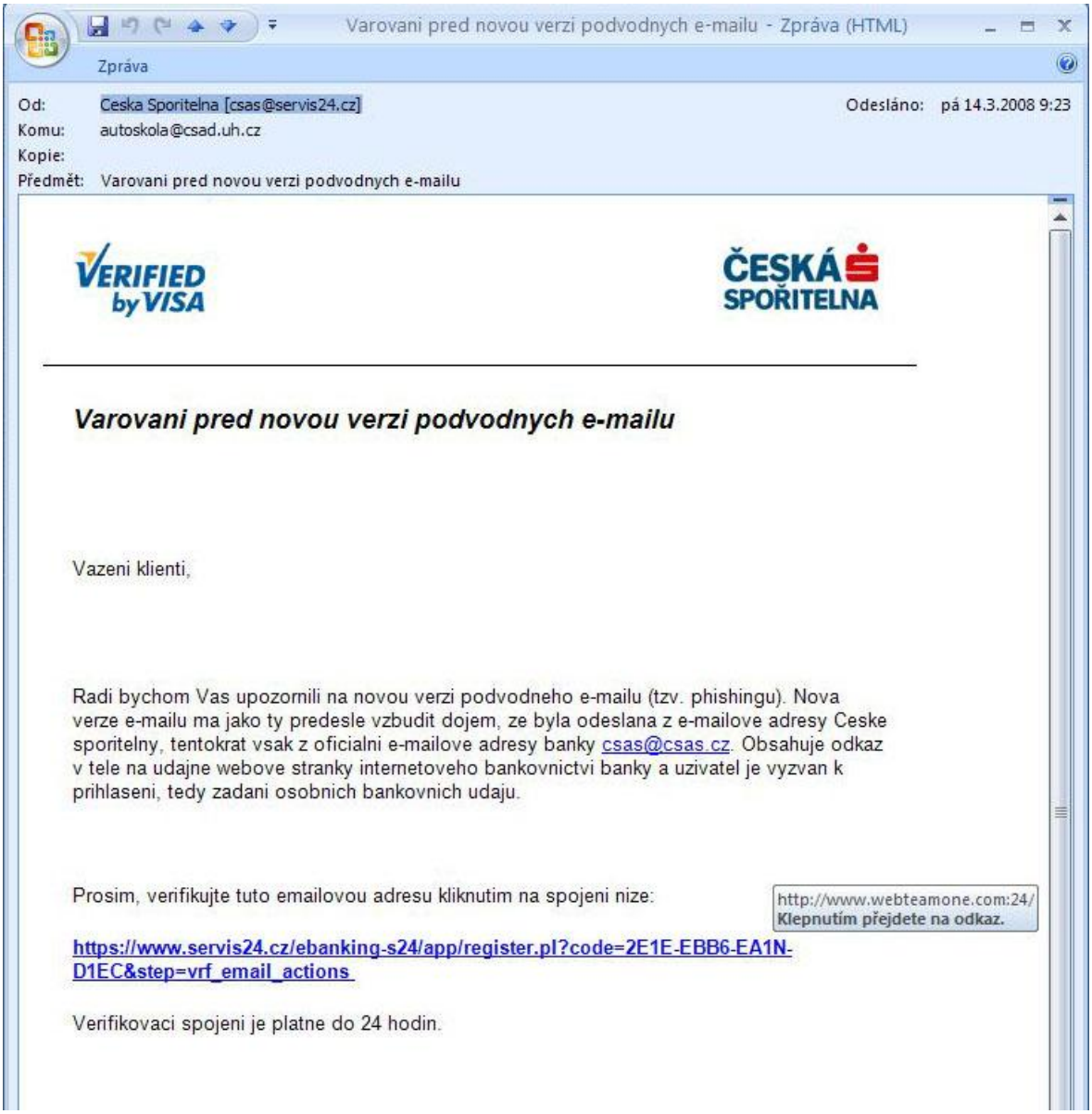
Opět zkomolená čeština, ale prokládána znaky azbuky.



Obrázek 9 – email z druhé vlny [zdroj: podvodný e-mail]

3.1.3 3. vlna

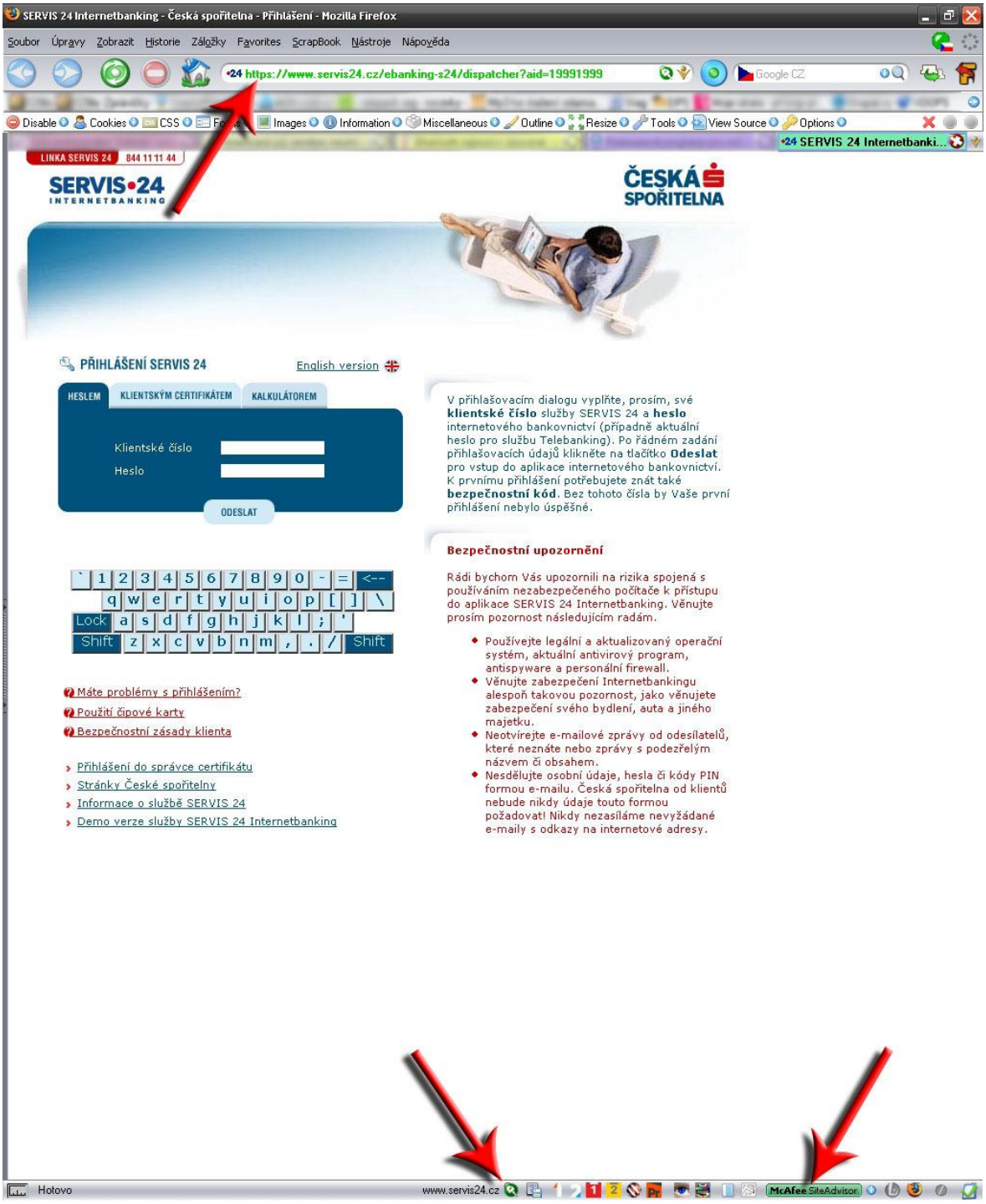
Velmi zdařená, podvodníci varovali před sebou samými, text byl bez interpunkčních znamének, ale psán byl spisovnou češtinou.



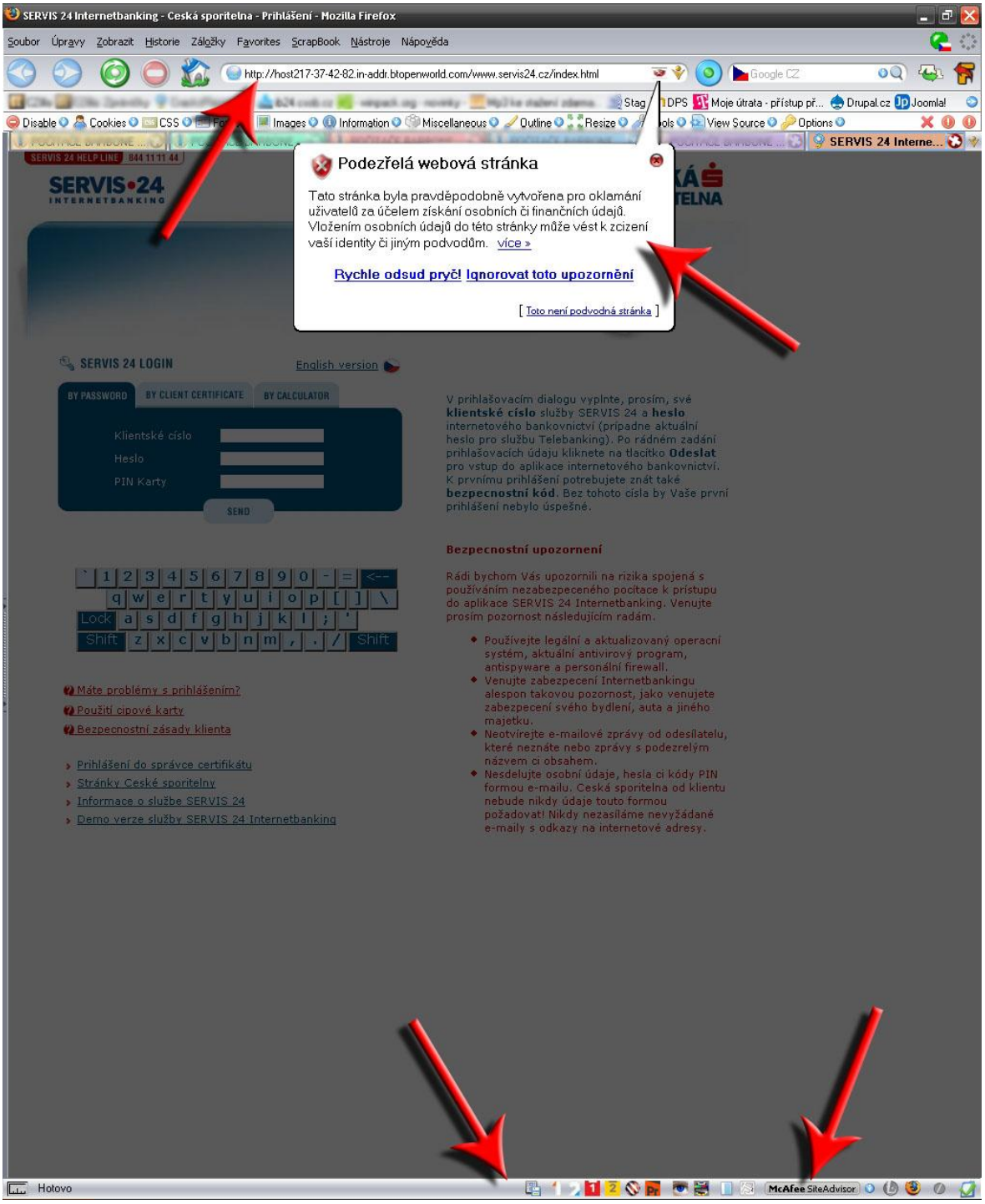
Obrázek 10 – email z třetí vlny [zdroj: podvodný e-mail]

3.1.4 Podrobný rozbor

Na následujících obrázcích si můžeme všimnout rozdílu mezi pravou a podvrženou stránkou. Podvržená stránka má v řádku s adresou pouze http místo https, chybí ikony zámků signalizující použití certifikátu a plugin (doplněk) prohlížeče nás varuje před podezřelou stránkou.



Obrázek 11 – pravá stránka České spořitelny [zdroj: www.csas.cz]



Obrázek 12 – podvržená stránka České spořitelny [zdroj: podvodný e-mail]

ZÁVĚR

Můžeme říci, že existuje možnost snížení nebo úplného vymýcení hrozeb, které na nás jako běžné uživatele číhají každý den na internetu?

Ano, existuje. Podmínkou ale je zásadní změna přístupu k jeho bezpečnosti. Proto v bankovnictví nejsou rozhodující délky šifrovacích klíčů nebo způsob tvorby elektronického podpisu pod platebním příkazem. Nejdůležitější je opatrnost nás, uživatelů.

Bezpečnostní systém může být nastaven tak, že v případě klientova přihlášení v neobvyklou dobu a přes IP adresy jiného poskytovatele připojení, se operátorům, kteří dohlíží na provoz, objeví tato operace jako podezřelá. V případě, že by se klient přihlásil přes zahraničního poskytovatele připojení a převáděl by částku vyšší než například 10 000 Kč, tak by byla operace automaticky zablokována.

Nemůžeme jednoznačně říci, že používání jména a hesla je nebezpečné. Stejně tak není správné tvrzení, že elektronický podpis nebo čipová karta jsou pro identifikaci osob vhodnější a více bezpečné. Zneužít je možné potvrzení bankovní transakce s pomocí jména a hesla, stejně tak je můžeme zfalšovat elektronický podpis nebo zneužít čipovou kartu. V prostředí sítě internet je nutné počítat s tím, že proti provozovateli internetového bankovnictví stojí profesionální počítačoví piráti, kteří se chtějí obohatit.

Závěrem lze konstatovat, že spoléhat se v oblasti identifikace klientů výhradně na technologie je velmi krátkozraké. Jak jsme se mohli přesvědčit v předchozích řádcích, postupy dnešních počítačových podvodníků to potvrzují.

ZÁVĚR V ANGLIČTINĚ

Can we tell that there is any possibility to decrease or entire removal treats, which are watching for common users on internet every day?

Yes, it is. The only condition is turning point access to its safeness. Therefore aren't decisive longitude encryption keys or way of production of electronic signature below payment order in banking. Most important is caution of us, users.

Security system is able to be set by so, that in the event of client's signing-up in unusual time and over IP address other provider of interface, operators, who overseeing running, discovers this operation like suspicious. In the event of client's signing-up over external provider of interface and transferring an amount superior to for example 10 000 CZK, operation would be automatically blocked.

We cannot tell that the using name and password is dangerous. As well is not correct statement, that the electronic signature or chip card for identification persons is more suitable and safer. It is possible to abuse confirmation of banking transactions with the aid of name and password; as well we can falsify the electronic signature or abuse the chip card. It is necessary to know that against the operator of Internet banking stay professional computer pirates, who want to enrich themselves.

In fine it is possible state that trust in the area of identification of clients entirely on technology is very short-sighted. How we could persuade in previous order, ways of today's computer cheats are bear to.

SEZNAM POUŽITÉ LITERATURY

Monografie:

[1] Lance, James. Phishing bez záhad. Praha : Grada Publishing, a.s., 2007. ISBN 978-80-247-1766-1.

[2] Matějka, Michal. Počítačová kriminalita. Prah : Computer Press, 2002. ISBN 80-7226-419-2.

[3] Smejkal, Vladimír. Internet @ §§§. 2. aktualiz. a rozš. vyd. Praha : Grada Puplishing, spol. s r.o., 2001. ISBN 80-247-0058-1.

WWW stránky:

[4] Anti-Phishing Working Group Phishing and eCrime Newswire. [Online] http://www.antiphishing.org/.

[5] Bednář, Vojtěch. Pharming je zpět a silnější. LUPA. [Online] Internet Info, s.r.o., 23. 3. 2007. http://www.lupa.cz/clanky/pharming-je-zpet-a-silnejsi/.

[6] Bitto, Ondřej. Rhybaření střídá pharming - LUPA. LUPA. [Online] Internet Info, s.r.o., 31. 03. 2005. http://www.lupa.cz/clanky/rhybareni-strida-pharming/.

[7] Bukač, Petr. Pozor na padělky! Měšec.cz. [Online] Internet Info, s.r.o., 19. 9. 2006. http://www.mesec.cz/clanky/pozor-na-padelky/.

[8] Matoušková, Ingrid. Časopis Policista č. 1/2006 - Právo a počítačová kriminalita. [Online] MVČR, leden 2008 http://www.mvcr.cz/casopisy/policista/2006/01/pockrim.html

[9] Džubák, Josef. Co je to phishing. HOAX. [Online] http://www.phishing.cz.

[10] Faturová, Marie. Podvodů s kopírováním bankovních karet přibývá - iDNES.cz. iDNES.cz. [Online] MAFRA a.s., 24. 10. 2007. http://ekonomika.idnes.cz/podvodu-s-kopirovanim-bankovnich-karet-pribyva-f5x-/ekonomika.asp?c=A071024_121835_ekonomika_maf.

[11] Fialová, Běla. Podvodníci zneužili bankomaty, tentokrát eBanky. Fincentrum.cz. [Online] MAFRA a.s., 12. 6. 2007. http://fincentrum.idnes.cz/fi_blind.asp?c=A070611_165623_fi_osobni_fib.

[12] Internetový magazín NaMíček. Kabinet Knihovnictvi. [Online] 18. 4. 2006. http://www.phil.muni.cz/vik/data/skyrik/namicek_1.pdf.

[13] Míra softwarového pirátství v Česku a ve světě – tisková zpráva. BSA - Business Software Alliance. [Online] 2007. http://w3.bsa.org/czechrepublic/statistiky.cfm.

[14] Mittelbach, Jan. Pharming může ošálit i zkušenějšího uživatele internetu. DigiWeb.cz. [Online] ECONOMIA a.s., 21. 3. 2008. http://digiweb.ihned.cz/c4-10146900-23480750-009000_d-pharming-muze-osalit-i-zkusenejsiho-uzivatele-internetu.

[15] Phishing (2). Security-Portal.cz. [Online] Security-Portal.cz. http://www.security-portal.cz/clanky/phishing-1.html.

[16] Phishing (1). Security-Portal.cz. [Online] Security-Portal.cz. http://www.security-portal.cz/clanky/phishing-1.html.

[17] Phishing - Wikipedie, otevřená encyklopedie. Wikipedie, otevřená encyklopedie. [Online] Wikimedia Foundation Inc., 13. 10. 2007. http://cs.wikipedia.org/wiki/Phishing.

[18] PhishTank > Statistics about phishing activity and PhishTank usage > April 2008. PhishTank. [Online] 5. 5. 2008. http://www.phishtank.com/stats/2008/04/.

[19] Phishing - Support. support.zcu.cz - server uživatelské podpory. [Online] Západočeská univerzita, 6. 3. 2008. http://support.zcu.cz/index.php/Phishing.

[20] Satrapa, Pavel. Phishing - nový trend v podvodných dopisech - LUPA. LUPA. [Online] Internet Info, s.r.o., 20. 05. 2004. http://www.lupa.cz/clanky/phishing-novy-trend-v-podvodnych-dopisech/.

[21] Turek, Rostislav. Keď platobnú kartu ktosi skopíruje. ŽIVĚ. [Online] Computer Press, s. r. o., 16. 5. 2008. http://www.zive.sk/default.aspx?article=277333.

[22] Samuelová, Katka. Bacha na skimming – i na vás může dojít!. ATLAS.CZ. [Online] ATLAS.CZ, 18.8.2007. http://podnikani.centrum.cz/ucty-karty/130454-bacha-na-skimming-i-na-vas-muze-dojit.aspx

Zákony:

[23] Zákon 140/1961 sb. ve znění pozdějších předpisů - Trestní zákon

[24] Zákon 121/2000 sb. ve znění pozdějších předpisů - Autorský zákon

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AOL America Online.

APWG Anti-Phishing Working Group.

ASCII American Standard Code for Information Interchange – americký standardní kód pro výměnu informací. Kódová tabulka, která definuje znaky anglické abecedy a jiné znaky používané v informatice.

BSA Business Software Alliance – protipirátské organizace.

CCV The credit card verification number – poslední tři čísla z kódu uvedeného na zadní straně karty.

CVC Card Verification Code – vyžadován při platbách po telefonu nebo Internetu.

DNS Domain Name Systém – je hierarchický systém doménových jmen.

FDI Fraudulent Device Inhibitor – bezpečnostní nástavec na bankomat.

IE Microsoft Internet Explorer – webový prohlížeč společnosti Microsoft.

IP Internet Protocol – jednoznačná identifikace konkrétního zařízení.

IRC Internet Relay Chat – chatování po internetu.

PHP Hypertext Preprocessor, původně: Personal Home Page

PIN Personal Identification Number – osobní identifikační číslo.

SMTP Simple Mail Transfer Protocol – internetový protokol určený pro přenos zpráv elektronické pošty (e-mailů) mezi stanicemi.

SSL Secure Sockets Layer – bezpečná (šifrovaná) komunikace klienta se serverem

TLD Top Level Domain – doména nejvyššího řádu.

URL Uniform Resource Locator – doménová adresu serveru.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK A GRAFŮ