On-line banking: Jak udržet peníze v bezpečí

Phishing, pharming, bezpečnostní mezery v bankách – nic z toho už není žádný problém. Náš speciální software vám peněžní převody na internetu kompletně zabezpečí. *Dominik Hoferer, autor@chip.cz*

V tomto článku najdete

Bezpečnostní balík pro on-line banking
Bankingový prohlížeč na bázi Firefoxu
Peněžní transakce s Linuxem na PC

Záměr je jasný: při internetovém bankovnictví musí vaše příkazy bezpečně dorazit k příjemci – bance. To ale není nijak snadný úkol, neboť na datové dálnici na vás číhá spousta nebezpečí. Nemějte ale obavy: Chip vám pro zabezpečení vašich peněžních transakcí nabízí hned dvě různé možnosti – všechny dobře „obrněné“, těžko prolomitelné a s individuálními přednostmi. Zde jsou programy, jimž můžete bez obav svěřit své peníze: exkluzivní prohlížeč pro internetové bankovnictví na cestách, zeštíhlený Linux pro vaše PC a bezpečnostní balík včetně firewallu pro komplexní zabezpečení počítače.

Základním předpokladem plynulého a bezporuchového toku peněz je „čistý“ počítač bez virů, červů a keyloggerů. K dosažení takového stavu vám pomůže bezpečnostní balík Chipu na přiloženém DVD, obsahující také firewall, SpyBot a virový skener.

Mobilní bankingový prohlížeč

Samozřejmě lze použít standardní browser a zabezpečit jej různými doplňky. Ty však většinou kazí požitek ze surfování, neboť standardně deaktivují skripty či spouštění multimédií. Mnohé webové stránky pak fungují jen omezeně, nebo nefungují vůbec. Řešením je druhý, speciální prohlížeč, určený pouze pro peněžní transakce. Nebo ještě lépe: varianta, kterou můžete mít všude s sebou. Tou je přenosný Firefox, dostatečně rychlý, štíhlý a malý, takže se vejde do USB paměti. Můžete si jej stáhnout z adresy **www.portableapps.com** a zabezpečit jej deaktivací všech pluginů. V krajním případě můžete použít verzi z Chip DVD, doporučujeme ale spíše návštěvu výše uvedeného webu, kde najdete nejnovější verzi. Počítejte

Bezpečné bankovnictví

S našimi nástroji vyřídíte své bankovní operace zcela bez starostí.

Bezpečnost na cestách

Firefox Portable
Bankingový browser, extra zabezpečený a přenosný

PhishTank SiteChecker
Ukáže, zda webová stránka není podezřelá

NoScript
Blokuje nežádoucí skripty

Zabezpečení pro domácí PC

VMware Player
Virtualizační nástroj pro bezpečné on-line bankovnictví

Damn Small Linux
Štíhlý opensourcový operační systém

Základní balík pro váš počítač

SpyBot – Search & Destroy
Najde v PC škodlivý software a odstraní jej

ZoneAlarm Pro
Firewall, který chrání PC před útočníky

AVG Anti-Virus plus Firewall 7.5 Chip
Ochrana před viry a vetřelci

však s tím, že na rozdíl od klasického prohlížeče v tomto případě „chybí čeština“ – jsou zde totiž k dispozici pouze čtyři jazykové verze (německá, anglická, francouzská, italská).

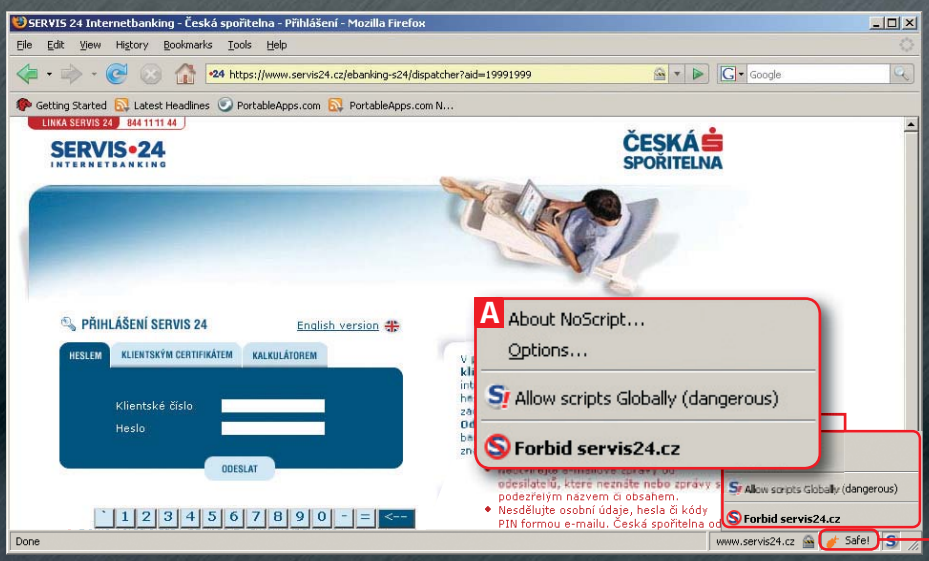
Postup jeho použití je následující: nejprve z webu stahněte exe soubor, ze kterého poté nainstalujete „portable“ Firefox na flash disk. Poté doinstalujte důležitá rozšíření a upravte nastavení browseru a můžete začít surfovat. V každém případě ale počítejte, že rychlost instalace na flash disk nebude závratná. Pokud se vám nechce „hrát si“ s různými rozšířeními a volbami, zvolte naši „Chip“ verzi, kterou najdete na našem webu.

V ní jsme předem nainstalovali nejdůležitější rozšíření a provedli jsme všechna bezpečnostní nastavení. Aplikace se spouští bez instalace, soubor jen musíte extrahovat. Na dalších řádcích vám krok za krokem vysvětlíme, jak jsme z Firefoxu udělali „hackeruvzdorný“ prohlížeč pro internetové bankovnictví. O odstranění slabin, které u něj odhalil test prohlížečů na straně 60, se starají vhodné nástroje a rozšíření. Zde se také ukazuje velká výhoda browseru od Mozilly: velká komunita programátorů pro něj neustále vyvíjí doplňky a ihned uzavře každou i dosud malou bezpečnostní mezeru.

Ochrana proti phishingu: Důležitým rozšířením pro bezpečné bankovnictví je PhishTank SiteChecker **(http://phishtank-sitechecker.com)**. SiteChecker vám ukáže, zda jste na webu cestou ke své bance nesprávně „neodbočili“ – a neskončili na nějaké phishingové stránce. Tato varovná funkce je aktivní po instalaci a restartu prohlížeče. Nástroj využívá výsledků spolupráce velké obce uživatelů, kteří podezřelé webové stránky okamžitě nahlašují. Jakmile se ocitnete na phishingové stránce, která už byla takto oznámena, SiteChecker vás o tom informuje. Mimochodem – potenciální phishingové stránky byste měli také nahlásit sami. Více se o tom dozvíte na webové stránce **www.phishtank.com.**

Zvýšení bezpečnosti: Nyní vhodným nastavením parametrů „opancéřujeme“ slabá místa prohlížeče. Například cookies by vždy měly být přímo vymazány při uzavírání Firefoxu – a to takto: v nabídce *Tools | Options | Privacy* v sekci Cookies by mělo být nastaveno „Keep until: I close Firefox“. Velmi nebezpečné je také ukládání hesel. Proto raději v kartě *Security* vypněte volbu „Remember passwords for sites“. Zadávat →

Bezpečné on-line bankovnictví – s námi doporučeným browserem

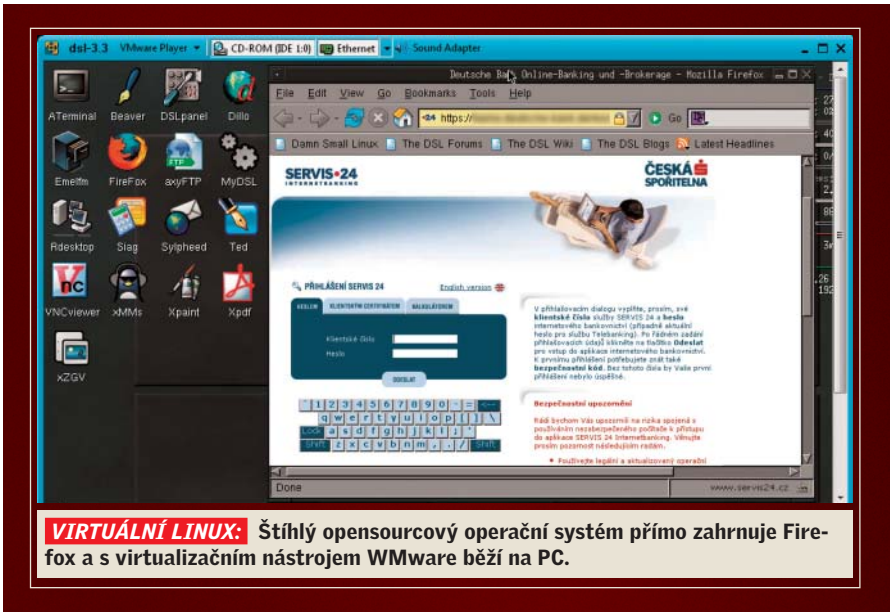


ŠTÍHLÝ A BEZPEČNÝ:

Chip doporučuje přenosný Firefox pro peněžní transakce na internetu.

A Rozšíření NoScript připouští JavaScript nebo multimediální soubory jen na určitých stránkách. To, které jsou důvěryhodné, určujete sami.

B PhishTank varuje před pochybnými stránkami, které ohlásila mezinárodní opensourcová komunita.



VIRTUÁLNÍ LINUX: **Štíhlý opensourcový operační systém přímo zahrnuje Firefox a s virtualizačním nástrojem WMware běží na PC.**

→ přihlašovací údaje pokaždé ručně je sice únavnější, ale pokud jsou tyto informace uloženy v prohlížeči, je zde nebezpečí, že je hacker dokáže přečíst.

Další krok: vypnout JavaScript! Tento skriptovací jazyk si oblíbili podvodníci – a správně navržená bankovní stránka funguje i bez něj. Prostřednictvím doplňku NoScript můžete určit, na kterých webových stránkách je JavaScript povolen a kde ne. Platí přitom základní pravidlo: Kde se zadávají citlivá data, tam skriptovací jazyk zablokujte.

A jak na to? Po instalaci se při surfování objeví u spodního okraje obrazovky lišta; po kliknutí na logo s písmenem „S“ zvolte položku *Options…* V menu, které se otevře, lze nastavit, pro které stránky bude JavaScript povolen (záložka Whitelist). Samotné zablokování je snadné – stačí jen kliknout na již zmiňované logo „S“ a zvolit zakázat „xxxxx.com“. Pokud ovšem bankovní stránka JavaScript potřebuje, musíte jazyk opět povolit.

Komu se nechce instalovat žádná rozšíření, může jazyk vypnout přímo v prohlížeči, a to postupem *Tools* | *Options* | *Content*. Zrušte zaškrtnutí u „Enable JavaScript“ a také u „Enable Java“.

Ovládací plocha: Jelikož je váš druhotný prohlížeč určen výhradně pro bankovnictví, měli byste jako domovskou stránku zvolit stránku své banky. Nejprve tedy tuto stránku otevřete a prostřednictvím nabídky *Tools* | *Options* | *Main* | *Use Current Page* ji prohlaste za domovskou stránku. Nakonec byste „bankovnímu“ browseru měli dopřát jeho vlastní ovládací plochu, abyste si jej nepletli se svým běžným Firefoxem a nedivili se pak, že některé webové stránky nefungují.

České internetové bankovnictví

Útoky na peníze jsou stále častější a zákeřnější. Jak je tomu ale u nás? Chrání nás čeština před největšími a nejzákeřnějšími ataky? *Petr Kratochvíl*

Neuplyne den, aby se v zahraničních médiích neobjevila zmínka o phishingových útocích na finanční instituce nebo o malwaru hledajícím přístupové údaje k bankovním kontům. V České republice jsou takové zprávy spíše výjimkou, skutečné případy ohrožení lze navíc spočítat na prstech jedné ruky.

Phishing

Oblast phishingových útoků je zářivou ukázkou výhodnosti našeho „exotického jazyka“ a počtu obyvatel. Zatímco naprostá většina uživatelů z okolních států musí při čtení mailů z banky alespoň trochu přemýšlet, u nás jsou phishingové útoky spíše zábavnou chvilkou při čtení nudné pošty. Jen málokdo by ze své skutečné banky čekal mail s podobnou perlou:

My ocenit tvuj obchod a clen urcity príležotost až k sloužit tebe.

Jak se zdá, pár set tisíc uživatelů s podivným jazykem plným exotických znamének zatím nestojí internetové mafii za námahu. Amatérské pokusy s automatickým překladačem jsou pro české uživatele spíše požehnáním, protože kromě zlepšení nálady pomáhají upozornit na existenci problému nazývaného phishing…

Malware

Mnohem horší je situace v oblasti malwaru. Tento škůdce totiž nezná hranice a je mu jedno, zda vyčmuchá heslo ve Francii, nebo v České republice. Pokud používáte svůj „surfovací“ počítač i k přístupu ke svému účtu, měli byste být opatrní. Za minimální opatření lze označit kontrolu alespoň před každým přístupem k účtu. Mnohem bezpečnější je však použití komplexního bezpečnostního balíku, který ve spojení s firewallem sníží riziko infekce malwarem na přijatelnou míru.

Obrana

Jak jsme se již zmínili výše, počítač sloužící k internetovému bankovnictví by měl být chráněn pomocí kvalitního bezpečnostního balíku. To ale nestačí. Mnohem důležitější je ochrana na straně

Jak to funguje v zahraničí

Některé zahraniční banky už používají moderní metody zabezpečení, výjimkou však nejsou ani „zajímavější varianty“. Poměrně rozšířená je například tato: po založení účtu a „zprovoznění“ internetového bankovnictví obdrží klient poštou PIN, na jehož základě si zvolí nový vlastní PIN. Ten může být snadněji zapamatovatelný, takže odpadají problémy s „hesly na papírcích“ nebo v souborech na ploše. V poště (nebo přímo v bance) klient dále obdrží list s padesáti autentizačními čísly (označují se jako TAN), kterými je nutné potvrdit každou transakci. Po provedení operace (a použití TAN) stačí příslušné číslo škrtnout a pro další operaci použít následující.

Perfektně chráněné domácí PC

Bezpečnostní systémy známé jako „security suites“ jsou důležité, bohužel však pro systém zároveň znamenají silnou brzdu. S Linuxem to jde lépe: v něm se obejdete bez antivirové ochrany i bez firewallu a v kombinaci s virtualizačním nástrojem VMware máte na PC kompletně odstíněný systém. VMware totiž používá pro webová spojení vlastní TCP/IP zásobník – tedy něco jako pancéřový vůz pro převoz peněz ve finančních službách.

Jako operační systém je vhodný Damn Small Linux (DSL), který dokážou snadno ovládat i začátečníci. Distribuce vyžaduje pouhých 50 MB na pevném disku a s virtualizačním nástrojem běží na PC bez problémů. VMware navíc spotřebovává tak málo systémových prostředků, že může trvale běžet na pozadí. Tento virtualizační program spustíte během několika sekund.

Instalace: Rozbalte „zazipovaný“ archiv DSL. V něm je obsažen ISO obraz a konfigurační soubor VMware nazvaný *dsl.vmx*. Nainstalujte VMwarePlayer. Pak postačí dvojité kliknutí na soubor dsl.vmx, aby nabootoval Linux. Při nabíhání ještě stiskněte Enter, a virtuální PC je připraven. Aby počítač běžel na pozadí a mohli jste jej rychleji spouštět, aktivujte ještě *VMwarePlayer | Preferences | suspend the Virtual Machine.*

Konfigurace: Máte-li ve své domácí síti DHCP router, dostanete se s nástrojem VMware na internet snadno bez konfigurování. Pokud surfujete přes modem, musíte ještě zřídit spojení. Probíhá to podobně jako pod Windows, údaje zadáváte do *System | Net Setup | dial-up PPP | config.* Damn Small Linux má jednu skvělou vymoženost: přímo s ním dostáváte i nejdůležitější program pro surfování – Firefox. Měli byste si jej však podle našeho návodu nakonfigurovat pro co nejvyšší bezpečnost.

Základní výbava Damn Small Linuxu umožňuje bankovní operace jen prostřednictvím Firefoxu. Chcete-li používat finanční software, jako je Starmoney, musíte si obstarat linuxovou verzi.

Dominik Hoferer

Tipy pro ještě vyšší bezpečnost

- Svá čísla kont a údaje PIN nikdy neukládejte v PC.
- Při bankovnictví přes browser vždy kontrolujte platnost bankovní adresy a dbejte na šifrování.
- U své banky si zřiďte pro platby denní limit. Kdyby se k vašemu účtu dostal hacker, způsobí pak jen omezenou škodu.
- Svůj účet kontrolujte pokud možno denně. V případě nesrovnalostí pak můžete banku ihned informovat a zabránit větším škodám.
- Po ukončení bankovní „seance“ se nezapomeňte odhlásit. Jinak by se hacker mohl prostřednictvím historie v prohlížeči znovu přihlásit – aniž by znal přístupové údaje.

banky. Naštěstí lze říci, že české banky patří v této oblasti ke špičce a zabezpečení internetového bankovnictví je až na výjimky na velmi vysoké úrovni. Pojďme se podívat na pár příkladů:

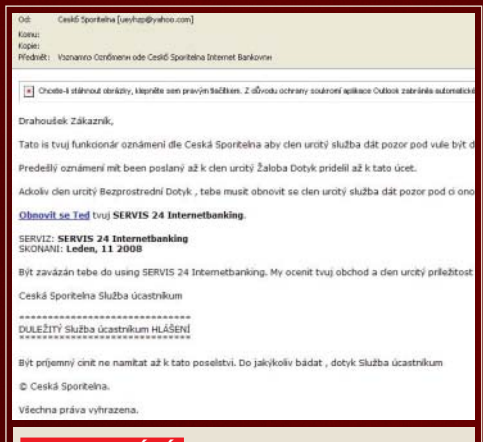
Jméno a heslo: Nejjednodušším a zároveň nejnebezpečnějším způsobem ochrany je kombinace uživatelského jména a hesla. Jejich získání je pro hackera obvykle snadnou záležitostí, a pokud jde o jedinou ochranu účtu, nestojí už „vybílení konta“ nic v cestě. Naštěstí se s touto samostatnou ochranou už téměř nesetkáte.

Certifikát: Mnohem bezpečnější je použití certifikátu. Banka vydá certifikát, který (pochopitelně po uložení na důvěryhodném médiu) slouží jako pojistka. Před připojením k účtu si totiž aplikace internetového bankovnictví zkontroluje, zda má uživatel platný certifikát. To spolu se zadáním hesla vytváří důstojnou ochranu před internetovými útoky.

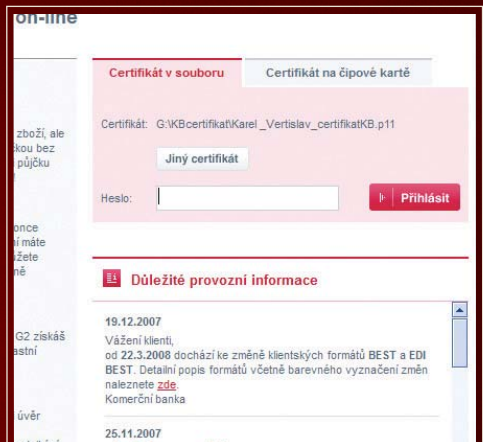
Extra PIN: Ještě lepší ochranou jsou prostředky umožňující generování jednorázových hesel. Tato zařízení (například PIN kalkulátor) umožňují kontrolu každé transakce, která na účtu probíhá. Modernější (a pohodlnější) variantou této ochrany je využití mobilního telefonu. Během zadávání transakce přes internetové bankovnictví je vám vygenerován jednorázový kód, který je odeslán na mobilní telefon.

Bude jen lépe

Většina českých bank používá kombinace několika výše uvedených metod, které ve spojení se standardními bezpečnostními prvky nabízejí dobrou úroveň bezpečnosti. Potěšitelné je, že se banky snaží pružně reagovat na nové hrozby ze strany internetových mafií. Klasickým příkladem je zavedení „grafické klávesnice“, na které zadáváte důležité údaje pomocí myši, a „klasické keyloggery“ jsou tak bez šance. I přes výše uvedené ochranné mechanismy lze při komunikaci s bankou doporučit zvýšenou obezřetnost. Jde přece o vaše peníze…



PRO ZASMÁNÍ: Pokusy o český phishing jsou zatím spíše komické. Stěží se najde někdo, kdo by podobné výzvě uvěřil...



CERTIFIKÁT: Zabezpečení přístupu k účtu pomocí certifikátu patří ke kvalitnější ochraně.