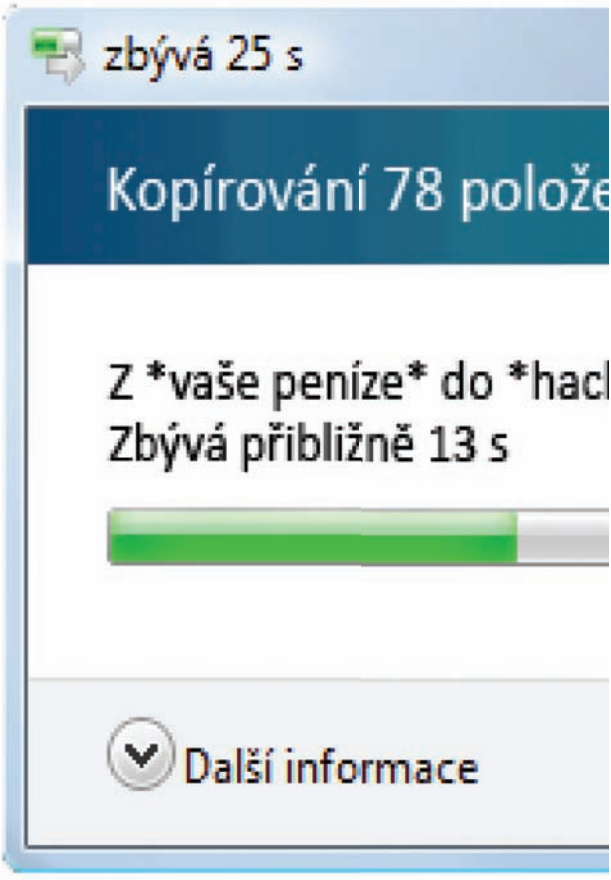
Nová rizika při on-line bankingu



Jedno špatné kliknutí a **PENÍZE JSOU PRYČ**. Ukážeme vám nejnovější pasti a nejčastější problémy, ale i to, jak bez obav surfovat prostřednictvím bezpečného browseru, který naleznete na Chip DVD.

DOMINIK HOFEREK, PETR KRATOCHVÍL

Radost z pořízení nového počítače byla obrovská. Prodejce ho nedávno připojil k síti a Dana V. hned chtěla prostřednictvím internetového bankovnictví zaplatit účet. Jakmile ale vložila kód TAN, na obrazovce se objevilo hlášení o chybě a stránka banky byla náhle off-line. Další šok přišel, jakmile se zkusila znovu nalogovat: podvodníci konto vykradli. Dana V. se stala obětí útoku označovaného jako pharming. Během několika minut hackeři zmanipulovali Internet Explorer takovým způsobem, že se místo bankovního portálu otevřela padělaná, podvodná stránka. Abyste měli jistotu, že jste před podobnými útoky chráněni a že vaše peníze dorazí na správné místo, pokusíme se popsat deset nejčastějších pastí, do kterých se můžete chytit při on-line bankovnictví. Ukážeme vám také, jak se před takovými nehodami chránit, a zároveň vám nabídneme perfektní ochranná opatření – náš bezpečný prohlížeč, který naleznete na DVD.

Pharming: Nebezpečná forma phishingu

Dá se předpokládat, že phishingu už moc lidí na lep nesedne. V dnešní době už jsou počítačoví uživatelé dobře informovaní a poučení, takže v e-mailech logicky nekliknou na linky, které vedou na bankovní stránky, a navíc existuje celá řada obranných mechanismů – od jednoduchých lišt a doplňků až po komplexní bezpečnostní balíky. Navzdory tomu všemu však phishing (v případě on-line bankovnictví) stále způsobuje největší škody. Internetová mafie ale nespí a vyvinula novou formu podvodu: pharming. Samotná past zde funguje trochu odlišně: malware ovládne vaše PC takovým způsobem, že vás prohlížeč dále navede na zmanipulovanou webovou stránku – přestože uvedete správnou adresu banky.

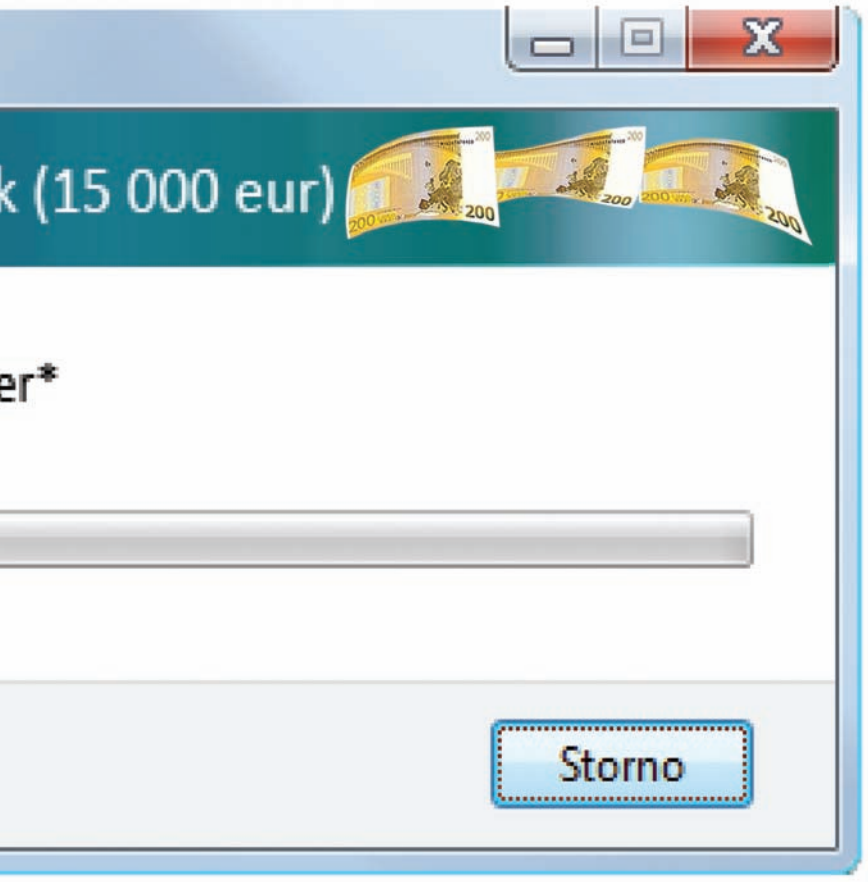
ŘEŠENÍ: Nejlepší ochranou proti pharmingu je update virového skeneru, protože ve většině případů je to právě malware, co stojí na počátku těchto útoků. Navíc si vždy zkontrolujte, zda URL bankovní stránky začíná „https“. Kromě toho se adresní řádek v nejnovějších browserech stínuje převážně do zelena či žluta a v dolní části browseru je zobrazen zámek, který informuje o šifrování. U mnoha imitovaných portálů tyto featury chybí. Dávejte si však pozor – přestože stránka obsahuje všechny náležitosti, může se jednat o zmanipulovanou stránku. Pokud má bankovní portál „cross-site script mezeru“ a hacker vytvoří phishingovou stránku, prohlížeč zobrazí všechny bezpečnostní pojistky.

V každém případě přijdete o peníze, pokud na pochybné stránce zadáte své přístupové údaje. Tam, kde hrozí phishing, je lepší URL banky vepsat manuálně, případně si v prohlížeči vytvořit záložku.

TRIK: Existuje jednoduchá metoda, jak odhalit falešné stránky: vložíte správné číslo konta, ale chybný přístupový kód. Pokud je stránka opravdu z vaší banky, obdržíte hlášení (zprávu o chybě), protože vstupní data si nebudou navzájem odpovídat. Zmanipulovaná stránka vám poděkuje za data, která jste vložili, a tato falešná data dále přepošle hackerovi, kterému však nebudou k ničemu.

Windows: Hodně slabá základní ochrana

Servery bank jsou ve většině případů z hlediska bezpečnosti téměř „neprůstřelné“. To však obvykle neplatí pro počítače uživatelů – alespoň pokud mají nainstalovaná Windows. Hackeři se tudíž místo útoku na finanční instituce stále častěji pokoušejí dostat k penězům přes nejslabší článek řetězce – přes počítače uživatelů. Aby byly šance podvodníků minimalizovány, Vista i XP vyžadují instalaci bezpečnostních nástrojů. Minusem ovšem bývá nezanedbatelné zpomalení PC a nutnost pravidelné údržby, tedy každodenního aktualizování antivirové ochrany!



RYCHLÁ POMOC

Správná reakce

Pokud se hororový scénář vyplní a vy se stanete obětí podvodu, dále vám pomohou následující tipy:

ZABLOKUJTE BANKOVNÍ PŘÍSTUP

První věc, kterou lze provést: zachovejte klid a zablokujte si bankovní operace. Denně si kontrolujte své konto, aby v případě, že by probíhaly nechtěné transakce, banka mohla hned reagovat a snažit se zabránit škodám.

KONTAKTUJTE BANKU

Pokud si jste jisti, že jste transakci provedli správně, ale stránka stále ukazuje nevysvětlitelnou chybu, ihned informujte svou banku – už to může být náznak činnosti hackera. I když vás to může vyvést z míry, snažte se být objektivní a zdvořilí a snažte se přesně popsat, co se stalo.

NEDĚLEJTE V PC ŽÁDNÉ ZMĚNY

Už se počítače ani nedotkněte a udržujte ho v nezměněném stavu. I když zjistíte, že máte v počítači trojského koně, nesnažte se tento malware odstranit. Nemohli byste tak zjistit, zda to, co způsobilo poškození, byl podvod.

ŘEŠENÍ: Nikdy na web „nevstupujte“ bez aktualizovaného antivirového softwaru! Ještě vyšší stupeň bezpečí však nabízí Linux. Díky našim „linuxovým řešením“ můžete dát sbohem zpomalujícím bezpečnostním programům, přičemž ale není nutné opouštět obvyklé prostředí Windows. Můžete používat oba systémy simultánně: bankovní operace můžete provádět pod Linuxem, úpravy obrázků a psaní textů pod Vistou a spol. Jednou z metod, jak toho dosáhnout, je použít Live CD jako např. Knoppix (více informací na **www.knoppix.org**).

Nevýhodou je, že svůj počítač musíte restartovat pokaždé, když se přepnete z Windows do Linuxu.

Můžete se také uchýlit k MokaFive Playeru (více informací na **www.mokafive.com**), což je virtualizér založený na VMwaru.

Výhodou je zde to, že lze jednoduše připojit Damn Small Linux. Je zhuštěný a pro bezpečnější on-line bankovnictví přímo nabídne Firefox.

NAJDETE NA CHIP DVD

Nástroje pro bezpečné bankovnictví

AVG Security Chip edition 08 ► Komplexní bezpečnostní balík

Avira AntiRootkit Tool ► Výborný antivir zdarma

Comodo Firewall Pro ► Kvalitní bezplatní firewall

NoScript ► Rozšíření pro Firefox

PhishTank SiteChecker ► Nástroj na obranu proti phishing

Spybot Search & Destroy ► Pomocník v boji proti malwaru

Chip Special

Nabízíme vám speciální Firefox Portable, připravený pro bezpečné surfování.

► **NA DVD:** Programy najdete na DVD pod indexem **INTERNET BANKING**.

Internet Explorer: Plný skulin

Fakt je, že Internet Explorer není zcela bezpečný. Program se spoustou děr a s ActiveX komponentami se sám nabízí k útokům. V srpnu tohoto roku nalezli bezpečnostní specialisté ze serveru Secunia v IE7 29 skulin, z nichž 10 představovalo bezprostřední riziko. Pokud i přesto chcete program používat, měli byste ho alespoň udržovat aktualizovaný.

ŘEŠENÍ: Mnohem méně šancí mají hackeři u Firefoxu, především pokud máte správná nastavení a aktualizace. Na našem DVD je pro vás připraven bezpečný prohlížeč – aktualizovali jsme totiž přenosnou verzi Firefoxu s nejdůležitějšími bezpečnostními plug-iny, čímž se tento nástroj stal ještě silnějším a bezpečnějším.

Integrovaný PhishTank SiteChecker ochraňuje před falešnými bankovními stránkami a varuje vás v případě, že se dostanete na nepravou webovou stránku. Plug-in má přístup do databáze, ve které má komunita seznam všech známých phishingových stránek.

Plug-in NoScript deaktivuje JavaScript, který může během bankovních transakcí představovat značné bezpečnostní riziko. Většina bankovních portálů navíc funguje i bez něj.

Výhoda navíc: browser se spouští přímo z přenosných médií, jako je USB flash disk nebo CD. Tento Firefox používejte na počítači jen pro peněžní transakce – navíc si v něm vytvořte link na bankovní stránku a své finanční operace provádějte pouze odtud.

TRIK: Pokud potřebujete relativně bezpečně surfovat po rizikových stránkách a poté manipulovat se svými financemi (aniž byste měli po ruce zmiňovanou přenosnou verzi Firefoxu), použijte Operu. Tento prohlížeč je díky svému relativně malému rozšíření mimo hledáček hackerů, proto ho většina nebezpečných skriptů číhajících na stránkách zcela ignoruje.

Otevřená síť: Pozvánka pro hackery

Nechráněná síť je nebezpečná a sama zve podvodníky, aby se k ní připojili. Nezáleží na tom, zda jste primárně připojeni bezdrátově, nebo přes kabel – špatně nastavený router a tím i otevřený WLAN vše hackerům ulehčují. Jediné, co „zloději" potřebují, je notebook a trocha času. Poté už vetřelec ovládá váš kompletní datový provoz – včetně podrobných informací o vašem on-line bankovnictví. I když ale nemáte bezdrátovou síť a připojujete se kabelem přímo k routeru, může mít toto řešení slabinu – standardní heslo. Doporučujeme ho co nejdříve změnit, protože vetřelci mohou jeho „pomocí" převzít kontrolu nad vaší sítí. Není totiž problém identifikovat model vašeho routeru přes podvodné stránky (pomocí JavaScriptu a Java Appletu) a poté získat přístup k routeru (a celé síti) pomocí jednoduchých nástrojů a standardního hesla, a to dokonce i z opačné strany zeměkoule.

Tento útok pak může být předehrou k útoku typu pharming, proti kterému již téměř není obrany. Po zmanipulování routeru (sítě) vám útočníci snadno podstrčí falešnou stránku banky, jako je tomu i u běžného pharmingu.

Problémem ovšem je, že zde vám už nepomůže žádný virový skener, protože útok probíhá i přesto, že na PC není zákeřný software nainstalován.

ŘEŠENÍ: Ihned změňte heslo svého routeru a použijte bezpečnou kombinaci čísel a písmen. Navíc přístup k WLAN musíte bezchybně zakódovat. WPA je nutností. Dodatečně zvyšuje bezpečnost i filtrování přístupu na základě MAC adresy (povoluje přístup k síti jen některým zařízením).

Zálohování přístupů: Značné riziko

I v těch nejbezpečnějších browserech se jednou za čas objeví skulina. Například ve Firefoxu 2.0.0.5 představoval riziko Password Manager. Jakmile uživatel aktivoval v prohlížeči JavaScript a uložil si přístupová data, útočníci byli schopni tato data na zmanipulovaných stránkách přečíst, nebo je dokonce přepsat.

ŘEŠENÍ: Vždycky mějte svůj prohlížeč aktualizovaný. Trhlina byla rychle odstraněna, což učinilo Firefox bezpečnějším, přesto se podobné riziko může kdykoliv objevit znovu. Nikdy si do počítače neukládejte citlivá data – především přístupové údaje do banky by vždy měly být vkládány manuálně.

Skladování TAN na PC: Žádná bezpečnost

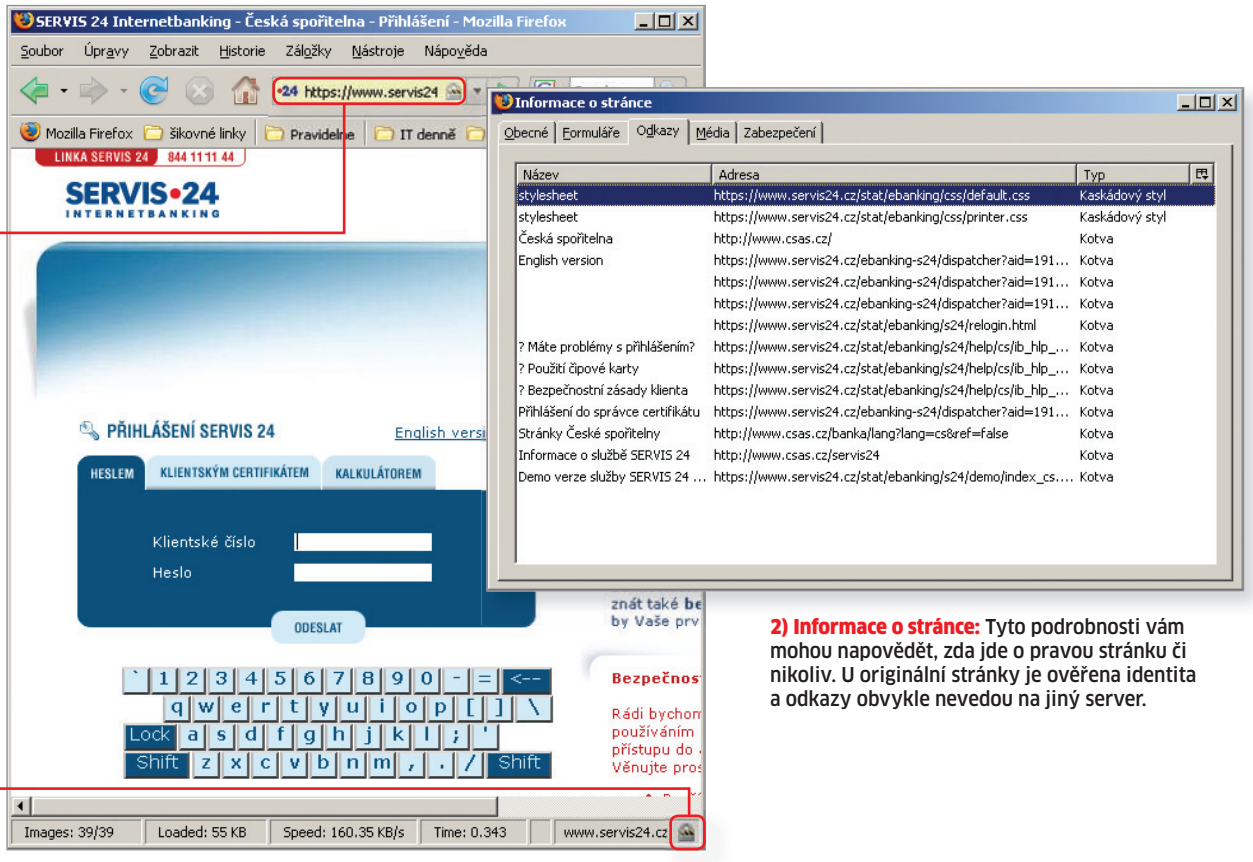
Pravidlo zmiňované pro přístupy je vhodné i pro transakční čísla. Dokonce ani datové sejfy nenabízejí kompletní ochranu před hackery. V našem testu „správců hesel" (v Chipu 05/08) jsme objevili skuliny ve dvou programech a hesla jsme dokázali přečíst. Vždy existuje nebezpečí: ochrana končí ve chvíli, kdy otevřete šifrovací program, abyste se dostali k údajům. Podvodníci dokázali v jednom zátahu přečíst obrazovku a získat všechna čísla TAN. Naštěstí je ochrana transakcí pomocí čísel TAN v našich bankách rychle vytlačována bezpečnějším potvrzováním přes SMS.

ŘEŠENÍ: Transakční čísla je nejlepší držet v šuplíku. Nebo ještě lépe – zažádejte si u své banky o bezpečnější proceduru ověřování transakce, a to o ověřování přes SMS. I když hacker získá přístup k vašemu účtu, bude si ho moci pouze prohlížet – jakýkoliv pokus o přesun peněz skončí neúspěchem a prozrazením...

Přehozené číslice: Vaše peníze jsou pryč

Malá chybička s katastrofálním důsledkem: spěcháte a potřebujete provést rychlý převod peněz, omylem však přitom přehodíte sousední číslice čísla konta příjemce. Banka odečte z vašeho účtu peníze jako obvykle, ty ale putují do rukou jiného příjemce.

Mnoho z nás neví, že jakmile je transakce ukončena, banka už nemůže přímo získat peníze zpátky (odebráním z účtu příjemce). Pochopitelně ve většině případů zaúřaduje smůla a číslo konta, které bylo špatně zadáno, opravdu existuje. To může být dost nepříjemné i tehdy, pokud okamžitě příjemce zažádáte o vrácení částky. V případě, že adresát není schopen



1) Proti phishingu: Moderní browsery už nabízejí ochranu proti phishingu v podobě barevně zvýrazněného adresního řádku.

2) Informace o stránce: Symbol zámku musí být zobrazen v této podobě. Po kliknutí na něj se zobrazí další důležité informace.

2) Informace o stránce: Tyto podrobnosti vám mohou napovědět, zda jde o pravou stránku či nikoliv. U originální stránky je ověřena identita a odkazy obvykle nevedou na jiný server.

platit a vaše peníze jsou pryč, zbývá jen soudní cesta…

ŘEŠENÍ: Jakmile data vložíte, pečlivě si zkontrolujte všechny detaily. Ještě jednou si je pak překontrolujte v okamžiku, kdy vás stránka požádá o potvrzení. Jakmile zjistíte nějakou chybu, ihned ji nahlaste bance.

Dobrá ochrana před překlepy: vytvořte si na bankovních stránkách vzory nejčastěji zadávaných platebních příkazů, a ty pak důsledně používejte. Tuto pomůcku nabízí téměř každá banka…

Operace s penězi na cestách: Riziková oblast

Pokud provádíte on-line bankovní operace v internetové kavárně, nemůžete si být nikdy jisti, že vaše peníze neskončí v rukou hackerů. Nikdy totiž nevíte, jak dobrá je antivirová ochrana počítače. Kromě toho je poměrně snadné v rámci sítě přerušit kompletní datový tok. Ve chvíli, kdy provádíte finanční operace, může hacker sedět vedle vás a vše nahrávat.

ŘEŠENÍ: Vyvarujte se transferu peněz přes neznámé počítače. Lepší variantou bývá tzv. „mobilní banking“, který nabízí mnoho finančních institucí za mírný poplatek. Pokud navíc potřebujete pracovat s penězi ze zahraničí, počítejte „u položky telefonní hovor“ s mírně vyššími náklady. I tak lze bez nadsázky říci, že i prozatím relativně vysoké částky za roaming jsou v porovnání se škodami, které může způsobit hacker, vždy nižší. Například v roce 2007 měl každý průměrný úspěšný útok hodnotu přibližně 4 700 eur.

Levný výdělek: Pozor na trestný čin!

V příkladu, který jsme uvedli na začátku, nemohl být hacker vystopován, protože ve hře ještě figuroval prostředník, který převedl peníze k hackerovi přes Western Union. Jen o několik minut později byl podvodník schopen převést obnos do kterékoliv banky na celém světě a k tomuto účelu potřeboval jen občanský průkaz. Ten ale bývá ve většině případů padělaný…

Další postup je logický – peníze jsou pryč a jediný, kdo může být obviněn, je právě tento pomocník. Jedná se většinou o důvěryhodného cizince, který naletěl na mail slibující obrovskou odměnu, když poskytne své konto k peněžnímu přenosu.

ŘEŠENÍ: Odmítejte podezřelé nabídky přes mail, které obsahují nespolehlivé sliby. Téměř vždy se za nimi skrývá nějaký podvod. Používejte přímé poskytovatele typu Western Union jen pro převod peněz lidem, které opravdu znáte.

Chybné odhlášení: Hrozné důsledky

Údaje pro převod jsou zkontrolovány, převod učiněn, ale místo abyste se metodicky odhlásili, jednoduše zavřete okno prohlížeče. Důsledky mohou být katastrofální, zvláště pokud jeden počítač sdílí několik lidí. Důvodem je i to, že na některých portálech je možné vyvolat bankovní stránky použitím historie prohlížeče a získat tak kompletní přístup k financím, aniž byste museli vložit PIN.

ŘEŠENÍ: Jediným řešením je správně se odhlásit. Pokud si přejete mít dodatečnou ochranu, všechny stopy zanechané browserem po bankovní operaci, jako je historie, cashe a cookies, vymažte. Bezpečný prohlížeč Chipu tohle vše provádí sám. Pokud i přesto uváznete v pasti nebo zjistíte nové metody podvodu, napište nám na adresu **redakce@chip.cz**.

AUTOR@CHIP.CZ