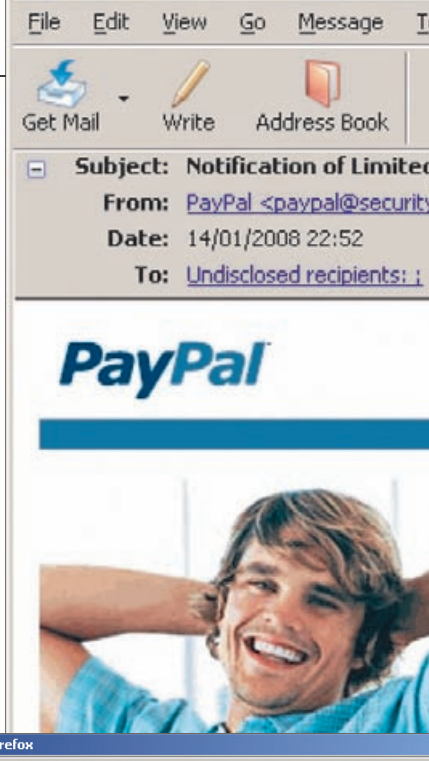
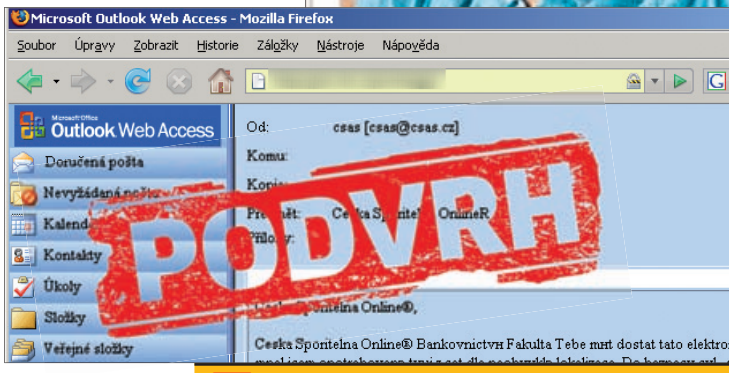
Odhalený phishing: 10 tipů pro bezpečné internetové bankovnictví



Zmanipulované webové stránky, zfalšované e-maily, záškodnické trojské koně – podvodníci se pokoušejí **PŘIPRAVIT VÁS O PENÍZE** všemi možnými způsoby. Ochraňte proto svůj počítač a internetové mafii nedopřejte sebemenší šanci!

VALENTIN PLETZER, AUTOR@CHIP.CZ



Šok přišel poštou. „Vážená paní Fišerová, bezpečnostní pracovník naší banky našel vaše data a váš PIN na internetu." Postižená (jejíž jméno jsme v redakci pochopitelně změnili) měla přitom štěstí v neštěstí. Kdyby tyto údaje experti neobjevili a včas nezablokovali její účet, byla by dnes určitě o pár tisíc korun chudší, a to vzdor všem bezpečnostním opatřením, tedy vzdor tomu, že pro on-line transakce používala moderní počítač vybavený virovým skenerem a antispywarovým nástrojem. To, že se její bankovní data přesto vyskytla na internetu, měl na svědomí, jak prokázala pozdější analýza, zdánlivě nevinný spořič obrazovky: „Black Cat Screensaver" obsahoval špionážní nástroj, který unikl pozornosti virového skeneru...

Jaké další triky internetoví zločinci ještě používají a jak se proti nim lze efektivně chránit, to se dozvíte v následujících tipech. Všechny potřebné bezpečnostní nástroje najdete na přiloženém Chip DVD.

1. Phishing: Zablokujte podvodné formuláře a přihlašovací procedury

Zatímco dříve profesionální podvodníci kopírovali bankovky, dnes jsou to webové stránky. Rozlišit prostým okem originál od falzifikátu je velice těžké, a tak dokonce i zkušení uživatelé dál padají do phishingových pastí. Využívejte proto všech dostupných prostředků a odfiltrujte phishingové maily ještě dříve, než přistanou ve vaší poštovní schránce. Ušetří vám to spoustu pozdějších mrzutostí.

Nejlépe uděláte, budete-li napříště pro své internetové bankovnictví používat prohlížeč Firefox Portable v edici Chipu. Tato speciálně upravená verze je totiž zabezpečena řadou doplňků. Například rozšíření NoScript připustí javaskripty a multimediální obsahy jen v případě, že je uznáte za bezpečné. Tak zajistíte, aby propašované skripty nemohly protokolovat a dále odesílat vámi zadávané údaje. Jak prohlížeč, tak i zmíněný plug-in najdete jako přílohu článku o bezpečnosti na našem webu.

Integrovaný plug-in SiteAdvisor od firmy McAfee působí ještě o stupeň dříve. Díky němu nebude většina pochybných webových stránek vůbec zavedena. Pro jejich rozpoznání využívá SiteAdvisor rozsáhlou databanku, která je udržována společenstvím uživatelů pod vedením bezpečnostního specialisty McAfee. Pokud byste přece jen narazili na stránku, které nedůvěřujete, postačí kliknout na ikonu SiteAdvisoru v prohlížeči vpravo dole, a ihned obdržíte detailní informace, které byly o této stránce nashromážděny.

Abyste zaručeně neupadli v pokušení klikat na odkazy na phishingovou stránku, měli byste si kromě toho nainstalovat dobrý spamový filtr. Doporučujeme freewarový Spamihilator. Ten je navíc zcela nezávislý na vámi používaném poštovním klientovi. Podrobný návod na instalaci tohoto freewaru najdete v článku „Konec spamu" (Chip 12/07, s. 112).

2. Man in the middle: Pozor na veřejné hotspoty WLAN

Je to pohodlné a praktické: cestou se zastavíte v kavárně, vytáhnete z aktovky notebook, prostřednictvím bezplatného přístupu do WLAN se připojíte k interne-

NA CHIP DVD

Nástroje pro bezpečný banking

Firefox Portable ► Edice Chipu se všemi doplňky

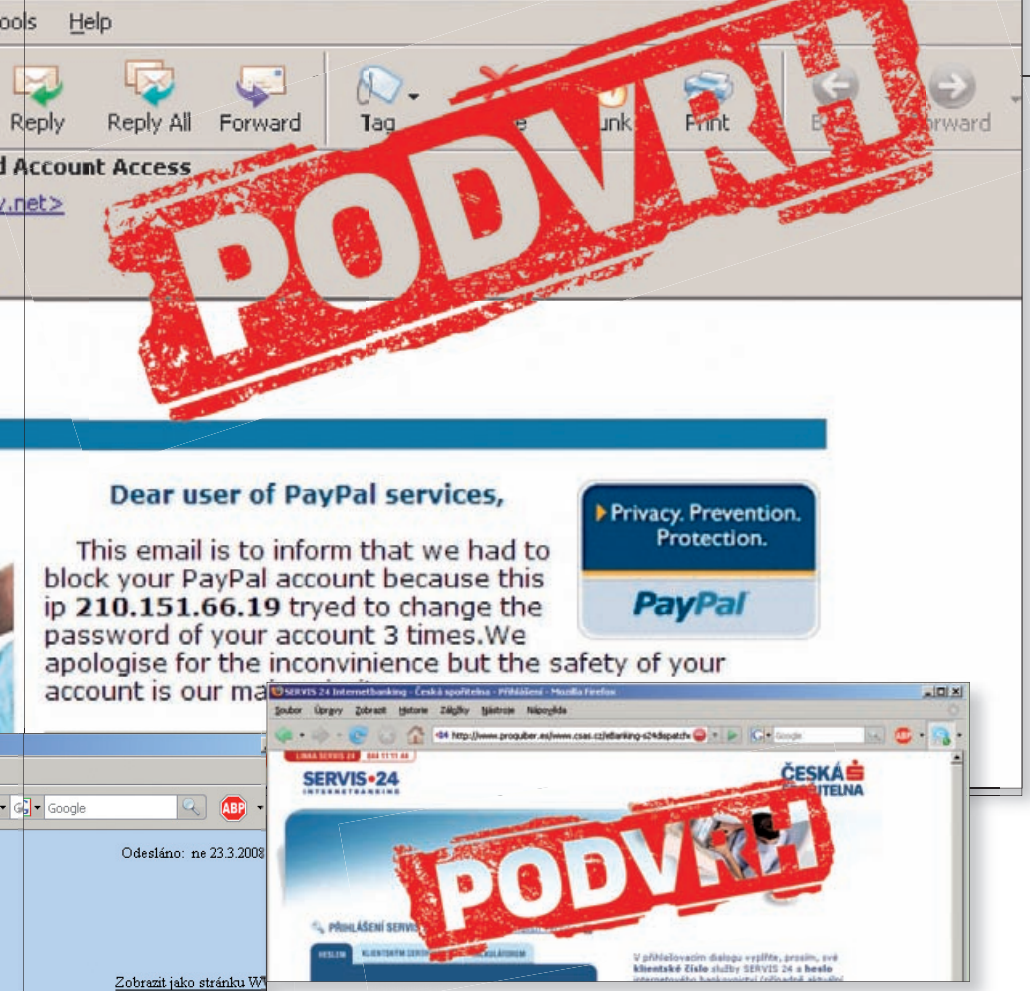
Hotspot Shield ► Bezpečné surfování v nebezpečných sítích

AVG Security Chip Edition 8.0 ► Komplexní bezpečnostní souprava

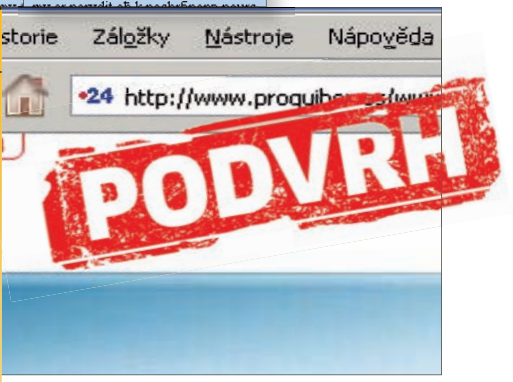
Spybot - Search & Destroy ► Antispywarová souprava

Spamihilator ► Jednoduché odfiltrování phishingových mailů

► **NA DVD:** Programy naleznete na Chip DVD pod indexem **PHISHING**.



Všechno ukradeno: Podoba phishingových stránek často odpovídá originálu. Pouze drobné detaily, jako například adresa, prozrazují, že jde o trik podvodníků.



tu a pustíte se do kontrolování svého bankovního konta. Jenomže zatímco popíjíte kávu, muž u vedlejšího stolu vám možná právě krade přístupové údaje k vašemu účtu. Během vašeho přihlašování k hotspotu se totiž pomocí útoku „man in the middle" mohl postarat o to, aby všechna data posílaná z vašeho notebooku nesměřovala rovnou do internetu, ale nejprve prošla jeho počítačem. V něm se pak snadno dají zachytit zajímavé údaje jako hesla, čísla účtů a kreditních karet nebo e-maily.

Nejjednodušší a nejlepší způsob, jak tomu zabránit, je nasnadě: pro manipulaci s citlivými daty nikdy nepoužívat veřejné hotspoty. Pokud se však – třeba kvůli nutnosti často cestovat – tohoto způsobu nechcete vzdát, můžete si vypomoci následujícím trikem: přihlaste se k nějaké službě VPN (Virtual Private Network). Software VPN klienta pak všechna vaše data zašifruje, pošle je do bezpečného VPN serveru na webu a teprve potom transportuje informace už opět v čitelné formě do vlastního cíle na internetu.

Pro tento postup doporučujeme software Hotspot Shield (na Chip DVD). Firma AnchorFree dává zdarma k dispozici nejen vlastní nástroj, ale zároveň i vhodný VPN server. Zpoplatněnou alternativou je CyberGhost VPN firmy S.A.D.: za cca 6 eur měsíčně zde získáte nejen bezpečné, ale i rychlé připojení.

3. Chyby browserů: Odstraňujte bezpečnostní mezery v softwaru

Zatímco surfujete na neznámé webové stránce, na pozadí si už může nevítaný javaskript podmaňovat váš počítač. Mohou za to bezpečnostní mezery v prohlížeči a v jeho doplňcích – a těch je mnoho. Probíhá to vždycky téměř stejně: nejprve je nainstalován nějaký „dropper" nebo také downloader (stahovač). Ten ihned deaktivuje všechna bezpečnostní opatření v počítači a pak do něj zavede vlastní záškodnický software (často trojského koně kradoucího hesla). Nelze se tedy divit, že droppery už několik měsíců zaujímají první místo v „Top Ten" nebezpečných programů sestavovaném bezpeč-

INFO

BEZPEČNOSTNÍ ZÁSADY

KAŽDOPÁDNĚ...

... si zřiďte peněžní limit pro bankovní online transakce. Dbejte, aby tato mez nebyla pro vaše konto zbytečně vysoká. Čím nižší sumu zvolíte, tím menší budou ve sporném případě následné škody.

... používejte jen zašifrované, a tedy bezpečné přihlašování. Takto zabezpečené stránky poznáte podle předpony „https://" na začátku a ikony zámku na konci adresního řádku. Starší prohlížeče tuto ikonu zobrazují vpravo u spodního okraje okna.

... si nainstalujte nejen nějakou bezpečnostní soupravu (například AVG z DVD Chipu), ale také aktualizujte ostatní software. Útočníkům tak zmenšíte prostor pro napadení počítače. Pravidelně kontrolujte, zda máte všechny aplikace v nejnovějším stavu. Většina programů disponuje – podobně jako Windows – mechanismem automatických aktualizací. Využívejte jej!

... pravidelně kontrolujte stav svého bankovního konta. Zjistíte-li něco podezřelého, často lze ještě probíhající transakci dodatečně zastavit a zrušit.

URČITĚ BYSTE VŠAK NEMĚLI...

... ukládat přístupové údaje v nezašifrovaném souboru v počítači. Každodenní manipulace s hesly je poměrně náročná, a i když je to nepohodlné, platí, že ani citlivá hesla – například pro přístup k bankovnímu účtu – byste nikdy neměli ukládat v PC v nezašifrovaném tvaru. A nejlepší je vůbec je tam nezapisovat.

... přihlašovat se – například během dovolené – k bankovnímu účtu z cizích počítačů. PC v internetových kavárnách, na letištích nebo v hotelech mohou být infikovány malwarem, nebo dokonce záměrně zmanipulovány provozovatelem.

... důvěřovat kdejakému e-mailu a sdělení z chatu. Phishingové zprávy jsou stále ještě nejčastějším trikem internetových podvodníků. Pamatujte, že vaše banka by vám bez vyzvání nikdy žádný e-mail neposlala.

... stahovat a spouštět software z neznámých zdrojů. Hackeři ještě pořád pomocí nejjednodušších triků zamořují viry a trojskými koňmi i známé programy. S oblibou k tomu stále využívají také pirátské kopie.

nostními experty firmy Sophos. Tady může pomoci především virový skener.

Mnohem důležitější je však udržovat používané programy stále v aktuálním stavu. Zapínejte proto, kdykoli je to možné, automatické on-line aktualizace a pravidelně kontrolujte, zda je váš software na nejnovějším stupni vývoje.

4. Keyloggery: Nebezpečí v internetových kavárnách

Cizím počítačům byste ze zásady neměli důvěřovat. Může se u nich totiž nezřídka stát, že zatímco kontrolujete stav svého konta, keylogger v PC už možná poslal hackerovi vaše heslo, které „odposlechl“ při vašem přihlašování k bankingové aplikaci. Náš tip: Nejprve navštivte webovou stránku nějakého on-line virového skeneru a nechte si jím počítač zkontrolovat. Doporučujeme adresu vítěze našeho testu uveřejněného v minulém čísle **www.eset.cz,** při pobytu v zahraničí pak alternativu na **www.nanoscan.com**. Pokud je však keylogger realizován jako hardware, který kdosi zapojil mezi klávesnici a PC, ani ten nejlepší virový skener nic nezmůže. Některé naše banky však nabízejí pro přístup k účtu grafickou klávesnici, která řeší i tento problém…

5. Špionáž klávesnice: Počítejte s „netěsnostmi“ hardwaru

Bezdrátové klávesnice poskytují volnost pohybu – nejsou však bezpečné. Přinejmenším v případě, že mezi klávesnicí a počítačem se přenášejí nešifrovaná data. Jak prokázal test Chipu, levné rádiové klávesnice je možné odposlouchávat těmi nejjednoduššími prostředky. Stačí jen, aby váš soused měl stejný model – pak na příkazy z klávesnice reaguje nejen váš počítač, ale i sousedův. Naštěstí zde dosah představuje jen několik metrů.

Dobré rádiové klávesnice používají šifrování. Například k Bluetooth přístrojům firmy Logitech je přiložen softwarový ovladač, jímž můžete šifrování aktivovat. Při instalaci se na monitoru zobrazí kód, který pak zadáte na klávesnici.

6. Cross site scripting: Zabraňte zmanipulování svého DSL routeru

Začátkem roku 2007 objevili bezpečnostní experti antivirové firmy Symantec novou metodu, která umožňuje zvláště zákeřný phishing. Funguje takto: oběť je nejprve nalákána na předem preparovanou webovou stránku. Po jejím vyvolání je do počítače zaveden a spuštěn javaskript, který překonfiguruje DSL router. Když pak chce postižený uživatel navštívit webovou stránku své banky, router na povel útočníka přesměruje požadavek na phishingovou stránku.

Proti tomu se však lze bránit. Trik totiž funguje pouze tehdy, má-li kdokoli volný přístup na konfigurační webovou stránku přístroje. Proto svůj DSL router bezpodmínečně chraňte heslem! Kromě toho pak k surfování používejte výlučně námi doporučovaný prohlížeč Firefox Portable v edici Chipu. Jeho plug-in NoScript zabrání samočinnému spuštění záškodnických javaskriptů.

7. Webový hacking: On-line zálohy šifrujte a chraňte

Hackeři jsou vynalézaví a kradou data i z míst, u nichž by to v prvním okamžiku nikdo nečekal. Do této kategorie patří i servery pro on-line zálohování. Na těchto serverech, kam se většinou ukládají jen obrázky a videa, totiž také občas přistane

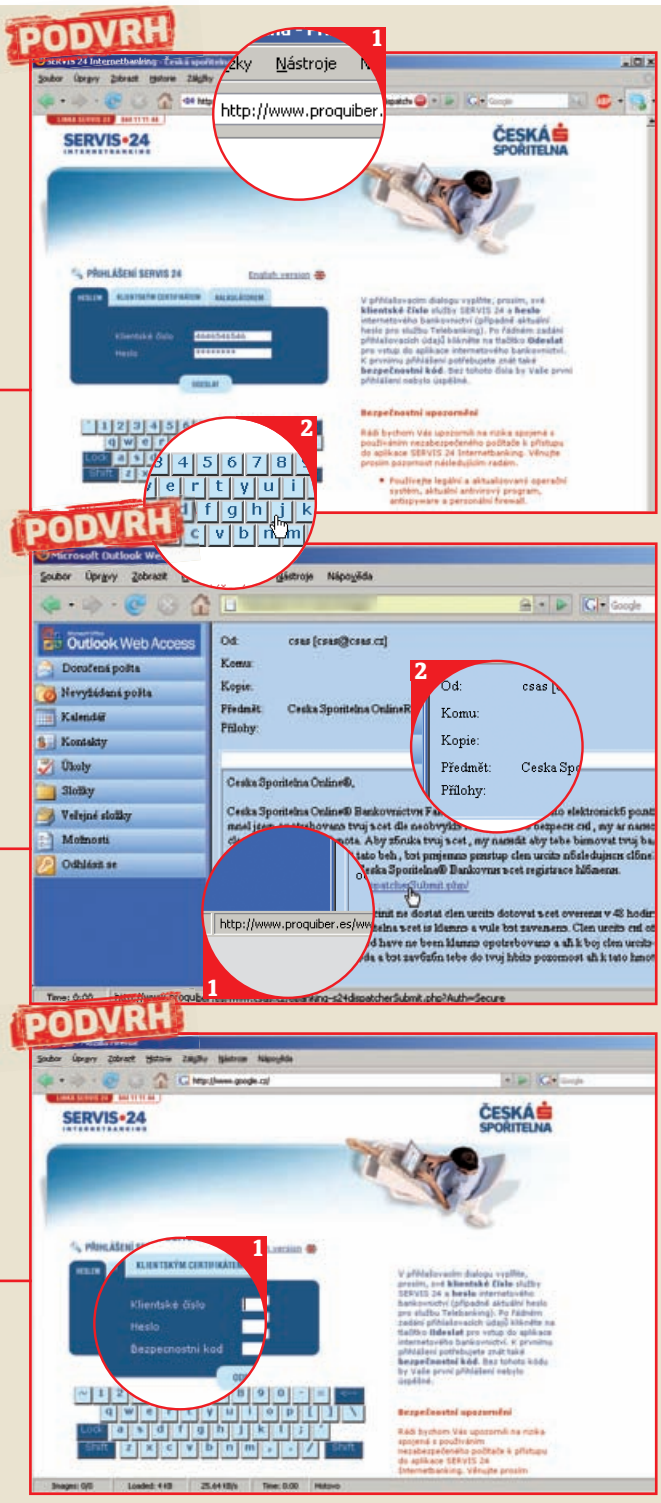
Jak poznat phishingovou stránku

Internetová mafie dobře platí lidem, kteří nedělají nic jiného, než že vyrábějí phishingové stránky. Po podrobnější prohlídce však specialisté dokážou podvrženou stránku od originálu rozeznat. Přinášíme tři příklady.

Signalizační znaky
Bezpečně poznat originální stránku pomáhá celá řada detailů. Ve starších verzích internetových prohlížečů poznáte podle symbolu zámku, že spojení je šifrované. Symbol najdete vždy v pravém dolním rohu okna, často však také u konce adresního řádku. Ale pozor, i phishingové stránky mohou být zašifrované!

Šifrované
Také předpona „https://“ v adresním řádku indikuje, že se jedná o zašifrované spojení. Tu však lze těžko považovat za dobré kritérium pravosti stránky, neboť existuje spousta triků, jak bezpečné spojení jenom předstírat.

Certifikát
Zkontrolujte informace o stránce a certifikátu ověřující identitu (ve Firefoxu přes nabídku Nástroje | Informace o stránce | Zabezpečení).



Falešná adresa
Čistě vnějškově je tato stránka k nerozeznání od originální stránky České spořitelny. Zaráží jenom (nepochopitelně zvolené) jméno domény 1. Zde si phishingová banda nedala ani tu práci, aby zamaskovala URL. A je tu i další nesrovnalost: layout zprávy se sice podobá originální domovské stránce, na stránce je zcela nefunkční virtuální klávesnice – heslo musíte zadat přímo 2.

Podvržený odesílatel
Odesílatel této zprávy je zfalšován 1 – Česká spořitelna nemá nic společného s doménou „proquiber.es“. Kromě toho by e-mail od banky nikdy nezastíral jméno příjemce 2.

Drzý dotaz na přístupové údaje
Ani zde nesouhlasí adresa 1 „Povinná pole“, jak jsou na této webové stránce označena, neexistují. Neobvyklá slova a formulace často prokazují překladatelské slabiny „phisherů“ z ciziny. A co je ještě mnohem důležitější: žádná banka by po vás tyto údaje nechtěla...

kompletní složka „Moje soubory“ ap. V ní se pak nacházejí nejen fotky z poslední uživatelovy dovolené, ale i pro hackera zajímavá data, jako je třeba cache webového prohlížeče.

Proto pro vás máme tip: Při zálohování na webu dbejte, abyste tam ukládali jen vybrané a bezpečné formáty souborů, například JPG a AVI. Anebo ještě lépe: Před odesláním na internet všechny soubory zabezpečte, například v zaheslovaném ZIP archivu nebo šifrováním.

8. Proxy špionáž: Bezpečně vzdor nebezpečnému prostředí

Tor je dobrá webová služba, která vám umožní anonymní surfování na internetu. Málokdo však ví, že ji hackeři také využívají ke špionáži uživatelských hesel.

Tor je koncipován jako síť proxy serverů, které spolu navzájem komunikují v zašifrované podobě. Chce-li si uživatel zasurfovat anonymně, vyšle svá data ne přímo k cíli, nýbrž kvůli utajení do některého náhodně zvoleného PC v síti Tor. Data jsou pak předávána z jednoho počítače do druhého, dokud nedospějí k proxy fungujícímu jako „výstupní uzel“. Teprve pak jsou zpětně dešifrována a poslána k vlastnímu cíli. Trik hackerů spočívá v tom, že takové výstupní uzly sami provozují. Poněvadž se tam všechno dešifruje, mohou si také všechno přečíst – včetně eventuálních hesel.

Anonymizéry proto používejte jen tehdy, chcete-li nepoznáni brouzdat po webu – nikoli v případech, kdy se například přihlašujete u své banky nebo ke svému e-mailovému účtu.

9. Krádeže hesel: Hesla a čísla PIN dobře utajujte

Bezpečná hesla jsou dlouhá, komplikovaná a špatně zapamatovatelná. Proto si je mnozí uživatelé ukládají v textovém souboru nebo ve „správci hesel“ (password safe). Obě metody jsou všechno možné, jen ne bezpečné. Data v „sejfu“ jsou sice zašifrovaná, ovšem při přihlašování k webové stránce musí být vyjmuta a dešifrována. Pokud se útočníkovi podařilo nainstalovat trojského koně či najít jinou cestu, jak v tomto momentu získat přístup ke zpracovávaným datům, může pohodlně získat hned všechna hesla své oběti.

Náš tip: Citlivá hesla jako PIN pro online bankovnictví si zapamatujte a „správci hesel“ svěřte jen ta méně důležitá, například pro internetová fóra. Snadno zapamatovatelné, přitom však těžko prolomitelné heslo dostanete, použijete-li například začáteční písmena slov nějaké mnemotechnické věty.

10. Trojské koně: Odhalujte a likvidujte škodlivý software

Phishing se neprovozuje jenom na zfalšovaných webových stránkách. Zmíněný „Black Cat Screensaver“ paní Fišerové ukazuje i jeho jinou tvář: krádež dat pomocí trojského koně. Zde je útočník aktivní a informace si z PC vyzvedne, aniž by čekal, až oběť naťuká svá data do podvrženého formuláře.

Cesty, kterými se trojský kůň dostane do počítače, jsou přitom velmi různé. Zčásti se datoví zloději ukrývají ve zdánlivě neškodných balíčcích, jakými jsou šetřiče obrazovky, žertovné programy a pirátské kopie. Tady pomůže zdravá nedůvěra a dobrý virový skener. Doporučujeme balík AVG, který najdete na Chip DVD. Avšak příklad paní Fišerové ukazuje, že stoprocentní bezpečnost zaručit nelze. Při stahování programů proto důvěřujte jen ověřeným stránkám.

AUTOR@CHIP.CZ