Prolomeno: Může se to stát komukoli

Hesla **CHRÁNÍ SOUKROMÍ** a důležitá data. Co se však stane, když je zapomenete nebo je někdo odhalí? Prozradíme vám, jak dostat zpět své dokumenty a posílit svou bezpečnost.

DOMINIK HOFERER

Něco je určitě špatně – Barack Obama nabízí poukázky na palivo, na Twitteru kolují špinavé drby o Britney Spears a na internetových fórech se objevil telefonní seznam Paris Hilton. Hackeři stále častěji útočí na přístupová data ke kontům celebrit.

Hesla ve světlech reflektorů

Útoky s cílem získat přístupové údaje k účtům jsou rok od roku intenzivnější, ale většina z nás si jich všimne, až když se obětí stane někdo známější. Pravda ale je, že oběti z řad celebrit v tom častokrát nebývají zcela nevinně: jejich hesla bývají často tak jednoduchá, že je hackeři odhalí bez větších potíží. Klasickým příkladem může být německý ministr vnitra, který zabezpečil svou webovou stránku použitím banálního hesla „gewinner“ (vítěz). Sarah Palin, kandidátka na viceprezidenta USA, nastavila bezpečnostní otázky ke svému kontu na Yahoo zadáním známých detailů ze svého života. Hacker na tyto otázky dokázal odpovědět s trochou „internetového výzkumu“ a poměrně snadno získal přístup ke schránce, přes kterou posílala i oficiální e-maily.

Ať už si o vztahu celebrit a počítačů myslíte cokoliv, jedno je jisté – obezřetnost při práci s hesly se nevyplácí podceňovat. Doporučujeme tedy používat dostatečně bezpečná hesla a pro každé z kont jiné heslo. Jak vytvořit bezpečné heslo a jak si ho také zapamatovat, to se dozvíte v rámečku na straně 103. Pokud se vám stane, že i přesto zapomenete své heslo k Windows, instant messengeru nebo PDF dokumentu, poradíme vám, jak ho získat zpět.

Pozor: Zmiňované aplikace používejte pouze pro získání přístupu ke svým dokumentům na vlastním počítači. Jejich jiné použití by mohlo být v rozporu se zákonem! Všechny zmiňované nástroje lze najít na našem DVD. Jako bonus jsme navíc

NA CHIP DVD

Bezpečnostní nástroje

Bart's PE Builder ► vytváří Windows-Live CD

Firefox ► browser s možností uložení hesel

FreePDF ► chrání PDF dokumenty pomocí hesla

Steganos Passwort-Manager Free ► umožňuje rychlé a bezpečné ukládání hesel

ImgBurn ► vypaluje „obrazy“ CD nebo DVD

KeePass ► nástroj na správu hesel

LastPass ► ukládá přihlašovací údaje pro Firefox a IE

Password Generator ► generuje bezpečná hesla

VMware Player ► simuluje virtuální PC ve vašem systému

► **NA DVD:** Programy k tomuto článku najdete na DVD pod indexem **HACKING**.

INFO

Snadné zapamatování hesel

Jednoduché pojmy jako běžná jména nebo často používaná slova příliš ochrany nenabízejí. Bezpečnostní expert Robert Graham analyzoval více než dvacet tisíc přihlašovacích údajů, které kolovaly po internetu během „hackerského procesu“ na fóru www.phpbb.com z počátku tohoto roku. A výsledek? Více než 94 procent hesel bylo snadné hacknout „hrubou silou“ pomocí slovníkové metody. Jedna třetina uživatelů použila jako heslo své jméno nebo vybranou sekvenci písmen na klávesnici (jako například QWERTY). S tím hackeři příliš práce neměli. Dobrým nápadem není ani nahrazování písmen abecedy pomocí čísel – například písmene e číslicí 3. I s tímto „trikem“ hackeři počítají. O dalších „špatných heslech“ jsme se zmiňovali v minulém čísle Chipu, kde jste mohli dokonce nalézt žebříček nejhorších hesel všech dob.

A jak lze hackerům ztížit práci? Používáním hesla obsahujícího kombinaci malých a velkých písmen, čísel a speciálních znaků. Jediným problémem tedy zůstává, jak si tento chaos zapamatovat. My vám ukážeme několik cest k bezpečnému heslu.

HLEDÁNÍ BEZPEČNÉHO HESLA:

První trik spočívá ve využití věty místo samotného slova. Pokud poté použijete v hesle první znaky z každého slova věty, vytvoříte kombinaci, se kterou si žádný hackerský software neporadí.

Příklad: Věta „V Brně jsem potkal 3 opilý kočky s Karlem v tramvaji číslo 12“ vytvoří heslo „VBjp3oksKvtč12“, které patří do kategorie „hackerova noční můra“.

Ideální samozřejmě je, pokud máte pro každou službu (nebo program) jiné heslo. Pokud už vám ale paměť příliš neslouží, zjednodušte si práci přidáním specifického řetězce. K výše zmiňovanému bezpečnému heslu si pro heslo na Seznamu přidejte „Sz“, u archivů rar zase „rr“ – zjednoduší to zapamatování a ztíží to práci hackerům.

Podobným způsobem si lze ulehčit i pravidelnou obměnu hesla – na počátek či konec přidejte kód pro vybrané období – mohou to být čísla 1210 pro prosinec 2010 nebo 04 pro poslední kvartál letošního roku – fantazii se meze nekladou. Pokud ještě přidáte speciální znak „+“, může vaše bezpečné „prosincové“ heslo na konto na Seznamu vypadat třeba takto: „VBjp3oks-Kvtč12+Sz+1210“. A s tím už si žádný hackerský nástroj neporadí…

přibalili Steganos Password-Manager, který dokáže vaše hesla bezpečně spravovat.

Prolomení hesla Windows a Wi-Fi ►

Nástroje: Tools: Offline NT Password & Registry Editor, Bart's PE Builder, Aircrackng

Superzabezpečení: Windows blokují přístup k vašim vlastním dokumentům, protože si už nepamatujete své přihlašovací údaje. Nemůže změnit nastavení své domácí sítě, protože jste zapomněli heslo (a nechce se vám resetovat router). Pomocí výše zmiňovaných nástrojů lze obejít vlastní bezpečnostní opatření a znovu získat přístup k domácímu operačnímu systému či k vlastní síti Wi-Fi.

UŽIVATELSKÝ ÚČET: Program Offline NT Password & Registry Editor vám pomůže tento problém rychle vyřešit. Resetuje totiž přístupové údaje k účtu na téměř všech systémech Windows – od Windows 2000 přes XP až po Vistu. Aplikaci lze najít i na internetu: je to 3MB „zip soubor", který obsahuje ISO image. Ten musíte vypálit na prázdné CD a získáte tak tzv. Live CD, pomocí kterého nabootujete svůj počítač. Postup je jednoduchý. Vložte CD do mechaniky, nabootujte počítač a software začne fungovat. Program má sice pouze textové rozhraní, ale do cíle vás snadno navede po jednotlivých krocích.

Upozornění: Aby systém nabootoval z optického disku, může být v některých případech nutné změnit bootovací sekvenci v BIOS ve prospěch CD/DVD mechaniky.

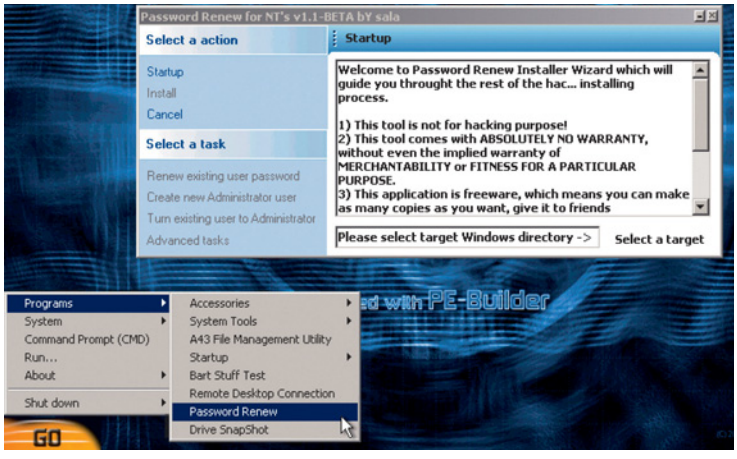
Pokud proti očekávání nástroj selže, existuje ještě další alternativa: Bart's PE Builder. Jeho instalace sice zabere nějakou dobu, tento program toho však nabízí mnohem více. Po malé úpravě ho spustíte také jako Live CD a dostanete Windows, která jsou spustitelná, uhlazená a rozšiřitelná použitím plug-inů. Pro použití programu Bart's PE Builder potřebujete i instalační CD Windows XP, výhodou je ale možnost přidání plug-inů k Live CD. Tyto plug-iny váš systém například opraví, zkontrolují, zda neobsahuje viry, či změní heslo.

FUNGUJE TO TAKTO: Na svůj počítač si nainstalujte Bart's PE Builder a z adresy **www.kood.org/windowspassword-renew/** si stáhněte program „Password Renew extension". Spusťte PE Builder (s právy administrátora) a vložte instalační CD Windows. Pak klikněte na tlačítko »Source«, zadejte cestu na CD/DVD s Windows a poté i požadovaná rozšíření přes tlačítko »Plugins«. Přes tlačítko »Add« integrujte do nástroje i program Password Renewer; tento plug-in se poté objeví na seznamu jako „sala's Password Renew". Stejným způsobem lze přidat a integrovat i jiné rozšíření. Nakonec okno zavřete. V nabídce »Create ISO image« zvolte cestu pro výstupní soubor a klikněte na »Start«. Výsledkem bude ISO soubor, který pomocí příslušného softwaru (například ImgBurnu z našeho DVD) vypálíte na prázdný disk. Poté počítač restartujte a do mechaniky vložte připravené CD/DVD (nezapomeňte také změnit bootovací sekvenci v BIOS). Při spouštění Bart's PE požádá o podporu sítě. Pokud chcete pouze změnit přístupové heslo do Windows, můžete klidně kliknout na »Ne«. Poté přes nabídku »Go | Programs | Password Renew« spusťte aplikace Password Renewer. Dále přes příkaz »Select a target« pátrejte po instalaci Windows, která bývá obvykle ve složce „C:\Windows". V nabídce „Renew existing user password" vyberte příslušné konto, změňte heslo a klikněte na »Install«. Po restartu budete mít opět přístup ke svému Windows kontu – ovšem s novým heslem.

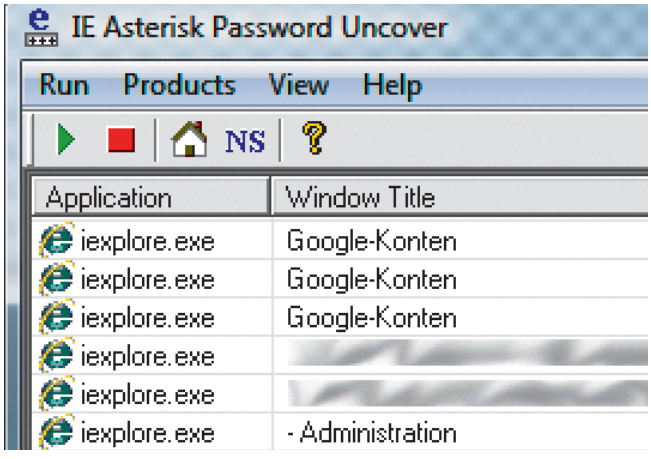
Jednoduché heslo, závažné důsledky

Často používáte jednoduché heslo, protože jste líní zapamatovat si složitější, navíc ho používáte pro většinu svých účtů. Jste ideální oběť hackera.

Ano, je to velmi pohodlné: přihlásíte se ke svému freemailovému účtu, pak použijete stejné heslo a zkontrolujete, co je nového na Facebooku, nebo odešlete pár zpráv přes Twitter a nakonec se stejným heslem přihlásíte ke svému „fotoúčtu" na Rajčeti nebo Picase. Myslíte si, že když vaše heslo hackeři odhalí, v podstatě se nic nestane? Hackeři mají celou řadu možností, jak vaše konta zneužít – odesíláním spamu počínaje, virovým útokem na jiné osoby zdaleka nekončě. Na první pohled neškodné, aktivní a „známé" účty jsou a v budoucnu ještě více budou hodně žádaným artiklem. Mnoho uživatelů také podceňuje další bezpečnostní mechanismy, které některé servery nabízejí. Ano, máme na mysli odpovědi na „kontrolní otázky", které vám mají umožnit přístup k účtu, pokud ztratíte heslo. Je obrovskou chybou používat v nich údaje, které může znát široký okruh známých, nebo které lze dokonce najít na internetu. Mít jako bezpečnostní otázku jméno svého mazlíčka (když jste se nedávno



Hacking Windows: Nepamatujete si heslo ke svému účtu ve Windows? Jednoduše změňte heslo v programu Bart's PE a pokračujte v práci...



Online data hacker: IE Asterisk Password Uncover zobrazí automaticky ukládaná přihlašovací data z Internet Exploreru jako text.

ve fóru několikrát zmínili, že musíte koupit Budulínkovi granule) je jako pověsit klíče od bytu na hřebík vedle kliky. Také dívčí jméno matky nebo vaše místo narození nejsou údaje, které by bylo příliš obtížné zjistit. Většina uživatelů si neuvědomuje, kolik soukromých informací o sobě prozradí i ve svém profilu na komunitní službě – a používat cokoliv z této oblasti k zabezpečení svého účtu je bezpečnostní sebevraždou. Pokud přesto potřebujete použít některou z „jisticích otázek“, upravte odpověď tak, aby ji nebylo lehké uhodnout. Například pokud je vaší oblíbenou barvou modrá, zadejte do kontrolní odpovědi „nebe“ (nebo „voda“).
V každém případě je ale mnohem lepší používat složitá a dlouhá hesla – návod na jejich vytvoření a zapamatování najdete na straně 103.

INFO

Politici pod palbou

Stejné pozornosti jako celebrity se mezi hackery těší i politici. Na to doplatila i ČSSD, která nedávno utržila ostudu s chybou XSS/HTML Injection, kdy nabídla své stránky jako vděčný cíl posměváčků (zkuste na Googlu zadat „čssd loupežníci“). O druhém selhání nedávno informoval webzin SOOM.cz **(www.soom.cz/index.php?name=articles/show&aid=509)**. Oficiální stránky politické strany chránilo heslo „xxx“.

WI-FI KLÍČ: Pokud se vám ztratila poznámka s Wi-Fi klíčem a zapomněli jste přístupové heslo k routeru, pomůže vám Aircrack-ng. Nezbytný předpoklad: Svou bezdrátovou síť jste si nezabezpečili pomocí WPA2 – pokud ano, nezmůže nic ani tento nástroj. Aircrack-ng pomůže pouze v případě ochrany pomocí WPA a WEP kódování. Nejjednodušší možností je spustit nástroj ve virtuálním stroji (například ve VMWare). Na webu **www.aircrack-ng.org** najdete pro virtualizér vhodný konfigurační soubor společně s instrukcemi, jak vám Wi-Fi „odemkne dveře“.

Odhalení: Program pro čtení hesel ►

Nástroje: Tools: IE Asterisk Password Uncover, Passwort Recovery, Asterisk Logger

Je to též praktické – jakmile jste jednou do browseru, instant messengeru nebo FTP klienta zadali a uložili své přístupové údaje, programy už tato data neodkryjí – vidíte pouze hvězdičky. Pomocí námi nabízených nástrojů však dokážete svá hesla znovu odkrýt – například pro jejich využití v alternativních programech.

PROHLÍŽEČ: Drobný pomocník s názvem „IE Asterisk Password Uncover“ rychle obnoví v prohlížeči uložená hesla. Práce s ním je snadná: spustíte nástroj, kliknete na malé zelené tlačítko v levém rohu a přejdete na přihlašovací stránku se zapomenutým heslem. Své heslo okamžitě vidíte v čitelné podobě.

Uživatelé Firefoxu žádný doplňkový program nepotřebují; mohou se totiž spolehnout na standardní nástroje prohlížeče. Všechna hesla uložená ve Firefoxu naleznete v sekci »Nástroje | Možnosti | Zabezpečení | Zobrazit hesla«.

Ale pozor – doporučujeme vytvořit ochranu hesel uložených v prohlížeči pomocí tzv. hlavního hesla, aby vaše data nedokázala přečíst třetí osoba. To provedete tak, že aktivujete zatržítko „Použít hlavní heslo”.

APLIKACE: Opět získat můžete i svá přístupová data k FTP serveru – i pokud se mail poskytovatele ztratil spolu s přihlašovacími údaji. Pomůže vám nástroj Password Recovery, který najdete například na adrese **www.reactive-software.com/ftp-password-recovery.html**. Pokud tento nástroj selže, můžete také vyzkoušet alternativní nástroj Asterisk Logger. Ten však funguje pouze ve Windows XP. Spusťte aplikaci, a jakmile otevřete program, ve kterém je uloženo heslo, logger (zapisovací nástroj) zobrazí přehled. Software najdete na **www.nirsoft.net**.

INSTANT MESSENGER: Pokud výše zmíněný nástroj selže ve vašem messengeru (například ICQ či Mirandě), zachrání vás MessenPass. Nástroj ukáže všechna přihlašovací data k účtům, která jsou v messengeru uložena. Stačí jen spustit nástroj, a zobrazí se všechny přístupové údaje.

SÉRIOVÁ ČÍSLA: Bez ohledu na to, zda používáte Microsoft Office, Photoshop, nebo software na úpravu videa, je postup při instalaci podobný. Po nainstalování programu musíte zadat příslušné sériové číslo. Pokud někdy musíte počítač reinstalovat a originální balení se sériovým číslem jste si někam založili, pak máte problém – tedy pokud nepoužijete nástroj „Magical Jelly Bean Keyfinder“, který může použít ke zjištění sériových čísel spousty běžných programů na vašem počítači. Tento program lze použít i ke zjištění sériového čísla vaší instalace Windows nebo klíčů pro Office XP, 2003 a 2007. Rozšířený konfigurační soubor stejně jako samotný software najdete na adrese www.magicaljellybean.com.

Odhalení skrytých textů ►

Nástroje: PDF Unlocker, Advanced PDF Password Recovery, Advanced Archive Password Recovery

Ti, kdo se obávají o své soukromí a chtějí si své dokumenty chránit, mají k dispozici celou řadu bezplatných nástrojů. Například pomocí freewarového nástroje FreePDF lze „zakódovat“ své PDF dokumenty a zabránit tak nepovolaným v jejich přečtení. Nepříjemná situace ale nastane, když po nějaké době zapomenete přístupové heslo a soubory se stanou nedostupnými i pro vás. Pomoc je ale na cestě: pomocí našich tipů můžete znovu získat přístup ke svým PDF souborům či heslem zabezpečeným archivům.

PDF: Můžete to zkusit například s nástrojem PDF Unlocker. Po instalaci najdete na ploše ikonu programu. Pomocí funkce „drag&drop“ přetáhněte „kódovaný“ dokument na ikonu a software vytvoří novou verzi PDF dokumentu (ve stejné složce, jako je originální soubor) – ovšem bez ochrany heslem. Pokud by byl program neúspěšný, můžete ještě vyzkoušet alternativní nástroj: Advanced PDF Password Recovery. Standardní verze tohoto programu stojí asi padesát eur, k dispozici je však i testovací verze zdarma. Tu najdete na webových stránkách autorů programu, tj. **www.elcomsoft.de**.

Upozornění: Nedělejte si zbytečné iluze o jeho schopnostech. Obecně lze říci, že program poměrně snadno otevře dokumenty, jejichž heslo není delší než čtyři znaky. Protože se program snaží zbavit ochrany použitím metody „hrubé síly“, může na pomalých počítačích zabrat odhalení delšího hesla dlouhé hodiny...

ARCHÍVY: Je praktické své ZIP či RAR soubory chránit heslem, protože pak můžete svá data zasílat mailem bezpečně nebo můžete lokálně zabezpečit vybrané celé složky před třetí osobou. V případě ztráty hesel pomáhá zpřístupnit dokumenty a jiné soubory program Shareware Advanced Archive Password Recovery. Nástroj opět používá metodu útoku „hrubou silou“ a v nabídce »Options« můžete určit, zda má nástroj pracovat s čísly a zvláštními znaky. Pokud jste ale nepoužili silné a komplikované heslo, jsou šance na opětovné získání přístupu k datům poměrně vysoké.

AUTOR@CHIP.CZ