Vážíte si svého soukromí?

Řiďte se našimi triky a ochraňte svá **SOUKROMÁ DATA** před zvědavými pohledy – a to jak na internetu, tak i na soukromém PC. Na našem DVD navíc najdete všechny důležité nástroje...

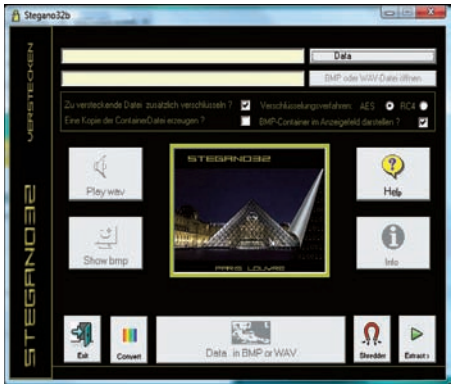
DOMINIK HOFERER

Zatímco čtete tyto řádky, mohou být již vaše data v hledáčku zvědavců. Mohl by to být malware nebo i váš šéf v práci, který chce vědět, zda v pracovní době nesurfujete po nevhodných webech. Nedávný skandál s ukradenými fotografiemi na komunitním webu Líbím se ti ukázal, že vaše soukromá data na internetu v bezpečí nikdy nebudou. Majitelé webu sice „ihned" přislíbili nápravu, pikantní fotky už ale kolují po internetu.

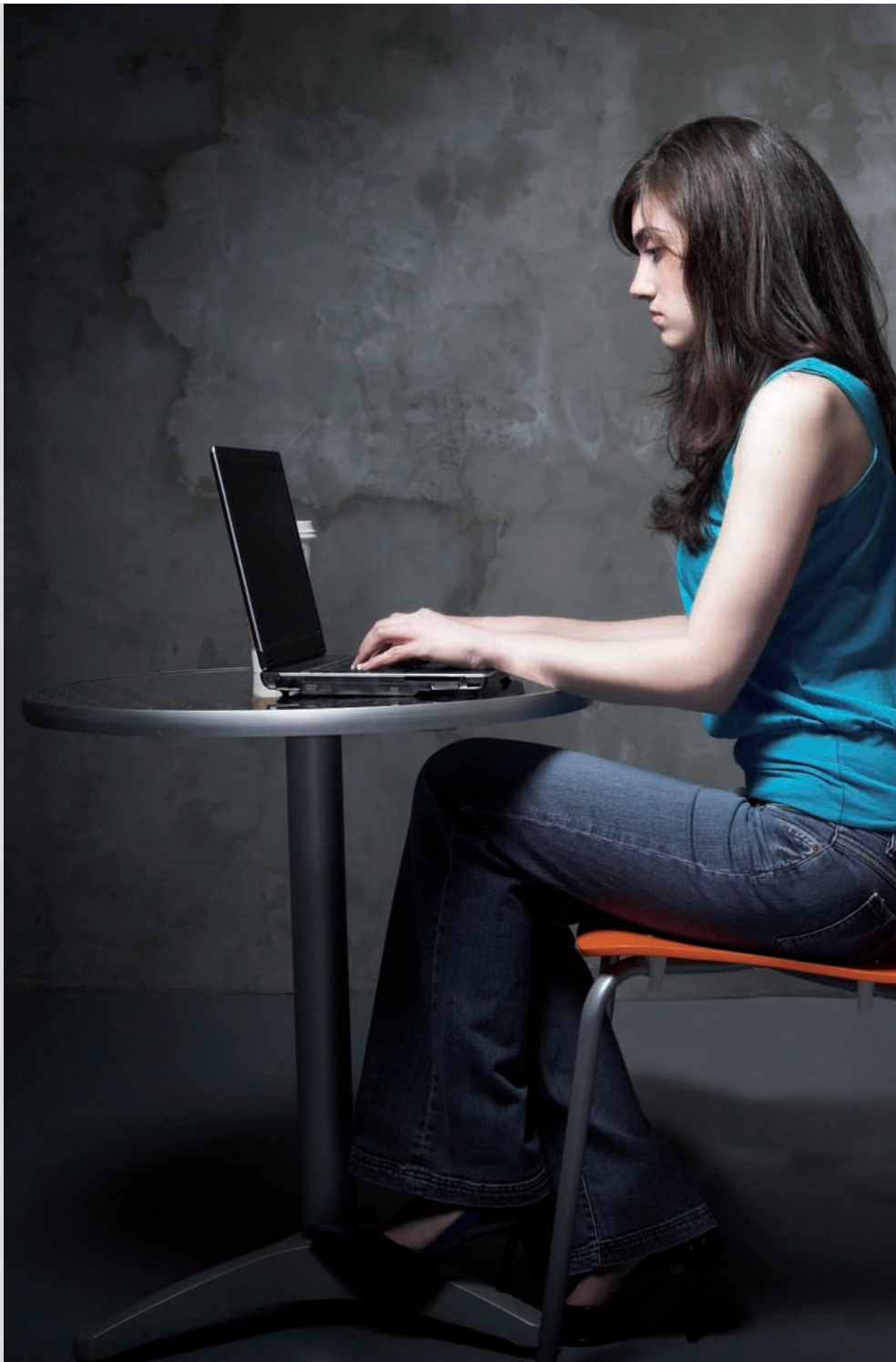
Místo abyste čekali, až webmasteři zlepší bezpečnost svých stránek, vezměte bezpečnost osobních dat do svých rukou. Ukážeme vám, jak ukrýt citlivé dokumenty i celé složky, jak anonymně surfovat na internetu a jak šifrovat tajné e-maily.

Obalamuťte špehy: Maskujte soubory

Nejste si jisti, zda váš kolega neslídí jako amatérský detektiv ve vašich souborech? Nejprve deaktivujte zobrazování naposledy otevřených dokumentů. To provedete tak, že kliknete pravým tlačítkem na nabídku »Start« a zvolíte položku »Vlastnosti«. Poté v okně »Upravit nabídku Start « klikněte na kartu »Upřesnit« a zde zrušte



Tajné: Program Stegano 32 dokáže skrýt data do obrázků a zvuků.

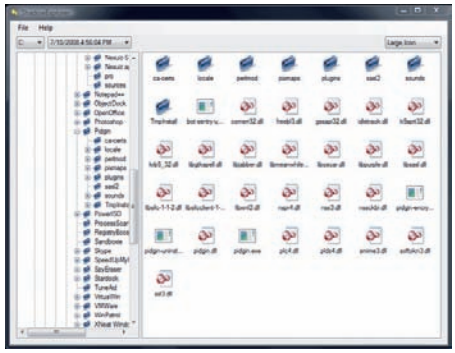


zatržítko u položky „Zobrazit seznam naposledy otevřených dokumentů“. Pokud váš kolega i nadále čmuchá okolo, sáhněte k dalšímu triku – ukryjte si data tak, že je nikdo nepovolaný neobjeví.

MASKUJTE JAKO OBRÁZKY: Fotografie z vaší poslední dovolené ukazuje pláž, palmy a moře. Náhodný pozorovatel však nevidí, že je toho v obrázku skryto ještě více. Pouze vy víte, že v obrázku je ukryta tajná powerpointová prezentace. A pouze ti, kdo mají správný program a znají správné heslo, mohou mít přístup k datům. Ostatní lidé vidí pouze plážovou idylku.

Technika skrývání informací do multimediálních souborů se nazývá steganografie. Data jsou uložena v souboru takovým způsobem, že se soubory jeví jako běžný obrázkový či hudební soubor.

TRIK: Poslední bit v bloku bajtů může být modifikován, a přesně sem může být tajný soubor „zapsán“ bit po bitu. Spusťte Stegano32b (najdete ho na našem DVD), který popsaným způsobem dokáže ukrýt jakýkoliv binární soubor. Po spuštění programu klikněte na »Hide file in a BMP image or WAV soundfile«. Jak už naznačuje jméno tlačítka, software může ukrýt vaše soubory pouze v jednom z multimediálních formátů. Na formátu ukrývaného souboru nezáleží. Nyní klikněte na »Open the file to be hidden« a pak na tlačítko »Open BMP od WAV file«. V jednom souboru můžete ukrýt téměř 10 MB. Když nahrajete soubor, který má být ukryt, nástroj zobrazí minimální velikost multimediálního souboru, který poslouží jako úkryt.



Shadow Explorer: Tento nástroj dokáže nejen odhalit data skrytá ve Windows Vista, ale také nabídne přístup k zálohovaným systémovým datům.

Výběr potvrďte kliknutím na »Hide file in BMP or WAV file«. Zadejte bezpečné heslo a nástroj přepíše váš BMP soubor a zamaskuje do něj vaše tajná data. Není se čeho obávat, stále můžete obrázek či WAV používat jako běžná multimédia – prohlížet je v prohlížeči obrázků nebo přehrávat v multimediálním přehrávači.

Pro obnovení souboru spusťte Stegano32b a zvolte »Extract previously hidden file«. Poté musíte zvolit „Open in Stegano Program“, zadat heslo a nakonec zvolit místo pro uložení.

UKRYTÍ DO ARCHIVU: Nevýhodou programu Stegano32b je fakt, že ho potřebujete i pro dešifrování. Například když posíláte soubor přes internet na jiné PC, nelze předpokládat, že by na něm byl tento nástroj nainstalovaný. V takovém případě zašifrujte tajný soubor pomocí „archivovacího softwaru“, jako je například 7-Zip, a standardního nástroje Windows. Pro „obnovu“ dat ze souborů je pak zcela dostatečný například i obyčejný Winzip **(www.winzip.com)**.

A jak to funguje? Po spuštění programu 7-Zip klikněte pravým tlačítkem na soubor, který chcete ukrýt. V kontextové nabídce jděte na »7-Zip | Add to archive«. Zde zvolte »Archive format | Zip« a nahrajte soubor. Nyní potřebujete obrázek ve formátu JPG. Na jeho velikosti nezáleží. Teoreticky platí, že do 30KB obrázku můžete schovat až 100 MB videa. Počítejte však s tím, že nový soubor zabere místo o velikosti objemu obou souborů. Nepříjemné také je, že velikost „obrázku” hned každého uhodí do očí.

A jak se data do obrázku dostanou? Pomocí příkazového řádku. Ve Windows XP klikněte na »Start | Spustit...« a do okna zadejte cmd. Objeví se okno s klasickým příkazovým řádkem, který již čeká na vaše zadání:

NA DVD

Bezpečnostní nástroje

7-Zip 4.57 ► archivační program
abylon BASIC 7.3 ► šifrovací nástroj
BeCyPDFMetaEdit 2.37.0 ► úprava pdf dokumentů
CyberGhost VPN Basic ► VPN klient
Enigmail 0.96.5 ► šifrovací doplněk
Exif Tag Remover 2.0 ► odstraňovač EXIF informací
GNU Privacy Guard (GnuPG) ► kryptografický software
Mp3tag v2.42 ► nástroj na úpravu mp3 tagů
My Lockbox 1.2 ► zamykání složek a souborů
ShadowExplorer 0.4 ► zpřístupní skrytá data
Firefox Portable Chip Ed. ► mobilní verze Firefoxu
Stegano32 v3.2 ► šifrovací nástroj
Steganos Safe One ► nástroj na archivaci
Thunderbird Portable ► přenosná verze emailového klienta
Tor 0.2.0.31 ► klient anonymizační sítě
TorChat 0.9.9.277 ► bezpečný komunikační program

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

```
copy /b obrazek + data.zip novy.jpg
```

Soubor „obrázek.jpg“ představuje obrázek, který poslouží jako úkryt, a „data.zip“ je váš tajný datový soubor. Po spuštění příkazu Windows vytvoří ve stejné složce soubor »new.jpg«. Pokud si kdokoliv bude chtít soubor prohlédnout, uvidí normální obrázek. Kromě velikosti nemusí nic naznačovat, že jsou v něm ukryta tajná data, a běžný obrázek jen málokdy vzbudí pozornost čmuchalů…

Chcete-li data získat zpět, změňte příponu souboru zpět z jpg na zip.

Pokud vaše Windows nezobrazí příponu, deaktivujte zatržítko v nabídce

»Vlastnosti složky | Zobrazení | Skrýt příponu souborů známých typů«.

Tato nastavení můžete obnovit po změně typu souborů. Soubor má nyní jméno data.zip a můžete ho otevřít jako jakýkoliv jiný archivní soubor.

Skrytí s poznámkovým blokem

Pokud na počítači nemůžete instalovat programy, Windows nabízí standardní nástroj k ukrývání informací i do běžného souboru. Jediné, co potřebujete, je poznámkový blok.

Otevřete příkazový řádek a vložte kód

```
notepad c:\data.txt
```

Následující zpráva o chybě indikuje, že tento soubor neexistuje, a systém se zeptá, zda ho chcete vytvořit. Klikněte na »Ano«. Vložte do souboru libovolný text a uložte ho. A nyní přichází trik. Znovu otevřete příkazový řádek a vložte příkaz

```
notepad c:\data:jmeno_souboru.txt
```

Opět se objeví zpráva o chybě. Tu znovu potvrďte kliknutím na »Ano« a vložte informaci, která nikomu nebude dávat smysl. Jakmile je soubor jednou uložen a ukončen, už se nikdy v Exploreru neobjeví. Jediné, co je možné vidět, je jmeno_souboru.txt; přiložený soubor data.txt viditelný není.

Abyste mohli znovu otevřít „tajný text“, musíte pouze opět použít výše zmíněný příkaz.

ÚSKALÍ: Zapomenete-li cestu a jméno souboru, je soubor ztracen – nemůže být přesunován či posílán.

Ochrana dat: Skryjte složku

Windows dokáží opravdu ukrývat složky i soubory. Ochrana ale není moc efektivní, protože dolní lišta v průzkumníkovi napovídá, že je přítomen „skrytý soubor“. Špeh pak může ukrytý dokument odhalit pomocí několika kliknutí.

My vám ukážeme, jak skrýt a zašifrovat celé složky.

SKRYTÍ SLOŽEK: Nástroj My Lockbox z našeho DVD vám ukrývání podstatně usnadní. Spusťte tento program a zvolte si heslo. Pomocí funkce drag & drop vložte do programu složky, které mají být ukryty. Poté vše potvrďte kliknutím na »Lock« a Windows složku skryjí. Složka se znovu objeví pouze tehdy, když spustíte My Lockbox a vložíte heslo.

Varování: Ve Vistě nabízí nástroj My Lockbox pouze omezenou ochranu. Nástroj Shadow Explorer, který najdete na našem DVD, dokáže skryté složky zobrazit.

Anonymita: Mazání stop

Nikdo není na internetu anonymní. Nezáleží na tom, zda pouze něco hledáte, nebo zda se snažíte stáhnout z pirátského serve-

Anonymní: Bezplatná verze programu Cyberghost surfování také zpomalí, ale to je jen malá cena za téměř dokonalou anonymitu.

Hledejte: Nástroj My Lockbox nabízí snadné ukrývání složek. Význam má ale především pro uživatele Windows XP.

Metadata: Zrádné informace

Fotografie, dokumenty ve formátu PDF i wordovské dokumenty obsahují více informací, než by se mohlo na první pohled zdát. Ukážeme vám, jak se jich zbavit…

Mnoho souborů, které na internetu zanecháváte nebo posíláte jiným osobám, může o vás a o vašem počítači odhalit celou řada detailů. Ukážeme vám, které nástroje a jaké triky dokáží vašim dokumentům „ulevit“ od zrádných metadat.

OBRÁZKY Ke každému zaznamenanému snímku přidává váš fotoaparát dodatečné informace o přístroji a jeho nastavení; EXIF data také mohou obsahovat jméno programu pro úpravu obrázků. Pro spoustu fotografů jsou tato data zajímavá a informují například o věcech, jako je doba expozice…

Ne každý však potřebuje vědět, jakou techniku používáte. **Exif Tag Remover** bez námahy odhalí (i odstraní) tyto informace, a to i při dávkovém zpracování.

PDF Dokonce i soubor ve formátu PDF si nese informaci o historii a původu. Například kdo soubor vytvořil, jak často byl soubor upravován a který program byl k vytvoření použit. Nechtěná metadata můžete ze souboru vymazat pomocí ná-

stroje **BecyPdfMetaedit**. Nahrajte do nástroje dokument a můžete vymazat všechna pole (Autor, Komentáře...).
WORD S odkazem na ochranu vašeho soukromí nabízí Microsoft nástroj, který je doplňkem Wordu a který dokáže odstranit metadata. Program **„Remove Hidden Data“** lze získat na adrese **www.tinyurl.com/5u33c**. Tento doplněk však funguje pouze v Office 2003.
V případě ostatních verzí budete muset příslušná metadata odstranit sami. Ve Wordu otevřete dokument a klikněte na »Soubor | Vlastnosti«. Zde v oddělených záložkách najdete informace, které potřebujete vymazat. Dodatečně také můžete vymazat některé osobní informace v nabídce »Nástroje | Možnosti« v kartě Informace o uživateli.

ru hudbu v MP3. Vaše surfování může být monitorováno. Chrome, nový prohlížeč od Googlu, vám nabízí téměř anonymní surfování pomocí funkce „inkognito“ (podobnou funkci nabízí i beta verze Internet Exploreru 8). I tak ale mohou být vaše kroky monitorovány softwarem třetí strany. Chcete-li se vyhnout i tomuto riziku, zkuste si nainstalovat program CyberGhost VPN z našeho DVD.

Tento nástroj při surfování nezanechává na internetu jedinou stopu a ve srovnání s jinými anonymizéry má navíc menší ztráty rychlosti. Oproti alternativě TOR& se program také mnohem snadněji instaluje a ovládá.

V bezplatné verzi (označené jako Basic) získáte měsíční limit 10 GB. Pokud chcete více, můžete si zakoupit verzi Premium, která stojí od 6 do 10 eur za měsíc, v závislosti na zvoleném tarifu. Po spuštění si nejprve musíte vytvořit nový účet – nebude vás to ale nic stát a zabere to minimum času.

Potom se přihlaste na server výrobce. CyberGhost ukryje vaši IP adresu a dá vám novou, pomocí které můžete surfovat, chatovat nebo sdílet své prázdninové video na P2P sítích. Pouze e-mailoví klienti jako Thunderbird nebo Outlook přes CyberGhost nedokáží komunikovat v zašifrované podobě. Abyste umožnili příjem mailů, musíte si v nabídce »Exceptions | eMails« zvolit svého mailového poskytovatele; běžní e-mailoví poskytovatelé jako Gmail jsou zde již přednastaveni. Nyní klikněte na »Status« a potom na »Connect Basic«. Během několika sekund nástroj vytvoří spojení se serverem operátora a vy dostanete novou IP adresu.

TIP: Z DVD použijte pro surfování náš „bezpečnostní prohlížeč“. Ten vás ochrání před phishingovými útoky, podvodnými stránkami a dalšími riziky internetu.

Soukromí: Šifrujte e-maily

Člověk by si mohl myslet, že e-mail je digitální forma dopisu. Toto přirovnání ale není zcela přesné – mnohem více „sedí“ srovnání s pohledem. E-mail je totiž podobně otevřený pro ostatní. Například téměř každý mailový poskytovatel využívá toho, že spam lze rozpoznat i přes automatické „skenování“ textu. Jak tedy e-maily ochránit, aby je nečetly cizí oči?

Nejprve potřebujete nástroj, který se jmenuje GnuPG a který také najdete na našem DVD. Jde o šifrovací systém, který funguje bezproblémově například i s Thunderbirdem. Technický proces šifrování mailů je následující: Vytvořte si soukromý a veřejný klíč. Veřejný klíč pošlete svému partnerovi, aby mohl dekódovat vaše e-maily. Soukromý klíč si uschovejte na bezpečné místo. A takto to funguje v praxi:

Jakmile po instalaci spustíte GnuPG, vyzve vás, abyste si vytvořili výše zmiňovaný pár klíčů. Budete ho potřebovat pro šifrování. Asistent vás provádí programem a požaduje informace, jako je jméno, e-mailová adresa a „heslová fráze“, což je ucelená fráze odlišná od normálního hesla, například „Richard z Yorku podstoupil boj zbytečně“. Vytvořte si zálohu kopie klíče a uložte ho na USB disk.

Abyste poslali klíč příjemci, klikněte na »Key | Export« a pošlete soubory lidem, kteří mají mít dovoleno číst vaše e-maily.

Teď si musíte nakonfigurovat svůj Thunderbird tak, aby automaticky šifroval e-maily. Z našeho DVD nejprve přidejte rozšíření jménem EinigMail a poté v Thunderbirdu v nabídce »Nástroje | Správce rozšíření« zkontrolujte jeho správnou funkčnost. Po restartu programu musíte Thunderbirdu prozradit umístění nástroje GnuPG na vašem PC. Proto hledejte cestu k souboru gpg.exe v nabídce »OpenPGP | Settings | Search«.

Nyní si pro sebe vytvořte testovací e-mail, klikněte na »OpenPGP« místo na Send. Při prvním použití si musíte nakonfigurovat svoji „identitu“. Potvrďte svou registraci a kliknutím aktivujte zatržítko „Enable OpenPGP support for this identity“. Po kliknutí na »OK« zvolte obě z horních možností v dalším okně. Nyní klikněte na »Send« a vložte svou heslovou frázi. Pokud jste dosud neposlali zašifrovaný e-mail příjemci, musíte nastavit pravidla pomocí příkazu „Set recipient rules“. Zvolte »Use the following OpenPGP key« a kliknutím na »Select« vyberte správné klíče.

Thunderbird nyní posílá váš e-mail a nikdo jiný kromě stanoveného příjemce nemůže vaši poštu číst. Vaše soukromá data jsou chráněna... AUTOR@CHIP.CZ

INFO

Průšvih jménem Líbím se ti.cz

Komunitní a seznamovací weby prožívají v poslední době velkým rozmach. Desítky tisíc uživatelů se zde baví, seznamují se i hledají práci. Kromě běžných a veřejně dostupných informací existovaly i informace, které byly přístupné jen po zadání příslušného uživatelského hesla. Vzhledem k tomu, že celá řada našich čtenářů má výborně zabezpečená data i na vlastním PC, jen málokdo by předpokládal, že si někdo může uložit na takovýto server něco „osobního“. Ukázalo se však, že tento názor je mylný – celá řada uživatelů (tedy přesněji řečeno uživatelek) si zde „volně“ uložila své intimní, často i erotické fotografie.

Další pokračování je už logické a bylo jen otázkou času, kdy k něčemu podobnému dojde: někdo obešel ochranu heslem a stáhl si téměř všechny „zajímavé“ fotografie. Neoficiálně jde o téměř 12 tisíc fotografií více než tisícovky dívek a žen, roztříděné podle jejich přezdívek na serveru. I přes počáteční naivní snahy administrátorů o zabránění jejich rozšíření je už na internetu můžete najít na celé řadě míst...

Celý příběh má ještě jednu pikantní rovinu – v celé řadě médií byl z ukradení fotografií nepřímo obviněn člověk s přezdívkou R.A.D.Y. Ten se ale brání tím, že jeho jméno se pouze objevilo na místě autora wordovského dokumentu se seznamem profilů s ukradenými fotografiemi. Je tedy vidět, že zapomenout vyčistit osobní informace z veřejně publikovaného wordovského dokumentu se vyplácí...

Psát, že pravého viníka už s největší pravděpodobností nikdo nevypátrá, je zbytečné. O své bezpečí se na internetu musíte postarat jen vy sami...