Anonymně na

Vyzkoušejte naše tipy a **OCHRAŇTE SI SVÉ SOUKROMÍ** nejen před slidivými pohledy – a to jak na internetu, tak i na domácím počítač. Na Chip DVD navíc najdete všechny důležité nástroje...

DOMINIK HOFERER

Pravděpodobně nejste ani tajný agent, ani na internetu nejednáte s islámskými teroristy. Nejspíš také na svém počítači nemáte „citlivé“ informace, kvůli kterým potřebujete šifrovat svá data pomocí nejdůmyslnějších metod šifrování.

Přesto lze na vašem počítači narazit na dokumenty, které je možné označit za osobní a u kterých by únik „na internet“ přinejmenším „nebyl žádoucí“...

Mohou to být výpisy z on-line bankovnictví, informace o daních nebo detaily z rodinného rozpočtu.

Jen málokterý uživatel by také ocenil, kdyby mohl kdokoliv zjistit podrobnosti o jeho toulkách internetem nebo dotazy, které zadá v Googlu. Proto vám ukážeme, jak surfovat na webu, aniž byste za sebou nechávali stopy, a také jak s co nejmenším úsilím na počítači ukládat soubory takovým způsobem, aby pro ostatní uživatele zůstaly nepřístupné. Jako obvykle pak všechny zmiňované nástroje, nutné k „vymazání stop“, najdete na našem DVD.

Bez výčitek svědomí: Surfujte s Firefoxem

Přestože se schopnosti Internet Exploreru s každou verzí rapidně zlepšují, stále ještě platí, že Firefox vás dokáže ochránit před útoky z webu lépe než konkurence od Microsoftu. Ale pozor, i Firefox za sebou zanechává stopy – pouze nabízí jednodušší a rozsáhlejší možnosti jejich eliminace.

Při běžném surfování mohou váš pohyb po internetu sledovat nejen správci navštívených stránek. Obvykle je sledován i váš pohyb po internetových obchodech – a to i v případě, že si žádné zboží nekoupíte. My vám poradíme několik triků, které o vás prozradí jen to nejnutnější.

NASTAVENÍ: Nejprve musíte v prohlížeči udělat několik málo změn. V nabídce »Nástroje | Nastavení | Soukromí« přejděte do sekce „Důvěrná data“ a zde klikněte na tlačítko »Nastavení«. Označte všechny položky, potvrďte kliknutím na »OK« a na závěr nezapomeňte aktivovat zatržítko u položky „Při ukončení aplikace Firefox vymazat důvěrná data“. Díky tomuto nastavení zmizí většina stop po surfování spolu s ukončením prohlížeče.

PC a internetu

Abychom však odstranili skutečně všechny stopy, musíme se podívat ještě hlouběji do konfiguračních dialogů. Kam tedy zajít, aby nebyly prozrazeny navštívené stránky a aby cíle vašich toulek internetem zůstávaly maskované?

Do adresního řádku prohlížeče zadejte příkaz

```
About:config
```

Pro zjednodušení hledání potřebné položky ještě do řádku „Filtr“ zadejte slovo „send“. Objeví se několik položek, nás ale zajímá pouze jediná: „network.http.send RefererHeader“. Dvojitým kliknutím ji otevřete a nastavte její hodnotu na „0“. Tím zabráníte správcům webu vysledovat, odkud jste se na jejich stránky dostali, tedy ani vyhledávací řetězec, který jste zadali do Googlu. Toto nastavení vám také pomůže s celou řadou „problémů“, které někteří správci webů připravují „cizím“ návštěvníkům (například při prohlížení obrázků).

ROZŠÍŘENÍ: Rozšíření Firefoxu CustomizeGoogle jde ještě o krok dál. Tento šikovný doplněk aktivně brání, aby si vyhledávače vytvářely váš přesný profil. Po instalaci ale musíte doplněk nejprve nakonfigurovat v nabídce »Nástroje | Nastavení CustomizeGoogle«.

Zde můžete například odstranit sledování myši, zbavit se otravných reklam nebo vypnout nápovědu Googlu. Další dvě volby důležité pro ochranu dat najdete v sekci »Soukromí«. Zde lze skrýt před Googlem svou identitu, stejně jako zakázat zasílání cookies serveru Google Analytics.

APLIKACE: Ještě mocnějším nástrojem z hlediska anonymního surfování je TOR. Zjednodušeně řečeno jde o „proxy“, maskující vaše stopy na síti a tím i vaši identitu. Používáte-li jej při surfování, ani správci webových stránek nebudou nikdy schopni vystopovat vaši opravdovou IP adresu, protože „od Toru“ dostanete novou.

Nejkomplexnějším způsobem maskování je zahalení se do neviditelného pláště pomocí kombinace programů Tor, Privoxy a Vidalia. To jsou nejdůležitější nástroje pro váš pobyt na internetu „beze stop“ – pokud je zkombinujete s Firefoxem, získáte snadný přístup k anonymnímu surfování. Balíček programů navíc k Firefoxu přidává tlačítko Tor, jehož pomocí lze jednoduše zapnout či vypnout proxy přímo z lišty prohlížeče. Při příštím spuštění už v pravém dolním rohu uvidíte, zda je Tor aktivován, nebo ne. Stav můžete změnit pomocí kliknutí pravým tlačítkem na ikonu Toru, čímž si rychle zajistíte anonymitu během surfování. Pokud chcete mít stoprocentní jistotu, navštivte například web **www.mojeip.cz**, kde se dozvíte svou současnou „identitu“ (například IP adresu a další informace o používaném softwaru). A protože proxy tuto informaci v nepravidelných intervalech „upravuje“, je téměř nemožné vystopovat vaše aktivity na síti. Cena za anonymitu však není zrovna malá: rychlost při surfování na webu je podstatně nižší. Podrobný návod na anonymní surfování najdete na našem webu na adrese **www.chip.cz**.

Další alternativou je nástroj CyberGhost. Přestože Tor zakryje vaše stopy lépe, aplikace CyberGhost nabídne jinou, pro celou řadu uživatelů důležitější výhodu: můžete surfovat podstatně rychleji.

Po nainstalování a spuštění programu si vytvořte na webu firmy (**www.cyberghostvpn.com**) zdarma účet a přihlaste se. V rámci bezplatného anonymního provozu máte k dispozici 10 GB dat na měsíc, což je pro běžné surfování více než dostatečné. Drobnou nevýhodou je ještě automatické odpojení po šesti hodinách provozu a negarantovaná rychlost. Ti, kteří potřebují více, si mohou objednat prémiové konto za přibližně 10 eur měsíčně (s datovým tokem 40 GB, minimální garantovanou rychlostí 2 000 Kb/s a 2GB online šifrovaným úložištěm). Avšak CyberGhost neumí jen „anonymní surfování“ – dokáže skrýt i váš „poštovní provoz“.

Neprůstřelná pošta: Komunikujte s Thunderbirdem

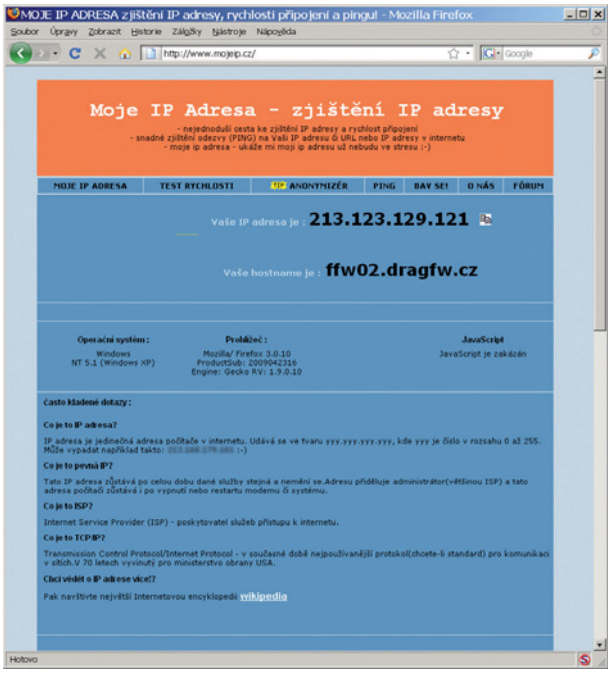
Existuje někdo, kdo má rád cizí lidi čmuchající v jeho soukromé poště? Většina běžných uživatelů se musí

NAJDETE NA CHIP DVD

Zabezpečení soukromí

CustomizeGoogle ► upravuje rozhraní a výsledky Googlu
CyberGhost ► maskuje vaši IP adresu
Enigmail ► zabezpečuje vaši elektronickou poštu
Gpg4win ► chrání soubory a složky heslem
GnuPG ► šifruje a podepisuje emaily
Mozilla Thunderbird ► alternativní poštovní klient
Prism ► nabízí pokročilou konfiguraci cookies
TrackMeNot ► nástroj na mazání stop
TrueCrypt Portable ► šifruje přenosné disky
Stegano32 ► skrývá dokumenty do multimediálních souborů
Steganos Shredder ► trvale odstraňuje data

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



Jste skryti: Na tomto webu si můžete ověřit, zda je vaše IP adresa skutečně změněna...

u mailů spoléhat na fakt, že poskytovatelé freemailových kont osobní maily obvykle nekontrolují. Existuje ale jiné riziko: vzhledem k tomu, že většina komunikace po internetu probíhá nešifrovaně, stačí, aby někdo „vyzkoušel“ zachytávání paketů na lokální síti příjemce nebo odesílatele, a cestu k obsahu vašich dopisů má volnou...

S Mozillou Thunderbird a novým rozhraním se můžete přestat tohoto rizika bát. Použijte nástroj GnuPG, který s Thunderbirdem bezproblémově spolupracuje. Stačí jen zařídit šifrování vašich mailů tak, aby zprávy mohl číst jen příjemce, a naopak abyste vám určené dopisy rozšifrovali jen vy. Kódování je asynchronní a funguje následovně: Pomocí GnuPG vytvořte sadu dvou klíčů; jeden bude osobní a ten druhý veřejný. Předejte veřejný klíč všem, od koho čekáte důležité e-maily. Zároveň si musíte dávat dobrý pozor na osobní klíč – nikdy byste ho neměli zveřejnit. To proto, že kódované maily odesilatelů můžete dekódovat pouze pomocí tohoto klíče. Podrobnější teoretické informace o této technologii najdete v minulém Chipu.

V praxi to funguje takto:

Na svůj počítač si nainstalujte GnuPG a k Thunderbirdu si přidejte doplněk Enigmail. V menu hlavního klienta klikněte na »OpenPGP | Key management«. V okně, které se objeví, přejděte na nabídku » Generate | New key pair« a zvolte ID (identifikaci e-mailového konta v Thunderbirdu).

Poté zadejte tzv. passphrase, což je (zjednodušeně řečeno) heslo, pomocí kterého se bude komunikace šifrovat (ideálně by se mělo skládat jak z čísel, tak z písmen). Toto „heslo“ si dobře zapamatujte, protože ho budete potřebovat k dekódování mailů. Profesionálové mohou ještě definovat sílu klíče v sekci „Advanced“ nebo zvolit speciální algoritmus. Nyní můžete vygenerovat samotné klíče (příkaz »Generate key pair«), což si ale vyžádá několik minut. Poté je váš poštovní klient připraven posílat utajené zprávy.

GnuPG vám nabízí dvě verze „lepší pošty“. První jen vylepšuje identifikaci: můžete zprávy podepsat digitálně. Díky tomu se může příjemce přesvědčit, zda byla zpráva opravdu zaslána vámi. Není to zbytečná práce, protože existuje celá řada metod, jak poslat mail vaším jménem (tuto technologii velmi často používají spammeři). Tomuto riziku se můžete vyhnout podepsáním svých e-mailů (v programu příkaz »OpenPGP | Sign message«). Jestliže příjemce vlastní váš veřejný klíč, Thunderbird potvrdí správného odesilatele a označí ho zeleným proužkem v horní části mailu. Pozor: Tento postup zprávu jen podepíše, ne zašifruje!

Druhá, bezpečnější a zároveň „nijak náročná“ varianta je zakódování odchozí pošty. Opravdu to není nic složitého – vyzkoušejte si to: Nejprve klikněte na »Compose«, poté klikněte na »OpenPGP | Encode message« a pošlete si mail. Zpráva by měla za nějakou dobu dorazit do vaší schránky. Zároveň by měl Thunderbird zeleným pruhem upozornit, že jde o „bezpečný e-mail“. GnuPG toho ale umí mnohem více – pomůže vám nejenom při kódování vašich mailů, ale i při šifrování lokálních souborů. Podrobnější informace najdete v programu v sekci „Secret“.

Tajný: Šifrování pomocí open-source

Ať už jde o telefonní účet, nebo o bankovní výpis stažený z portálu banky, papír postupně mizí z našeho běžného života, v současné době jsou důležité dokumenty stále častěji zasílány ve formátu PDF. Často pak leží nechráněné v počítači a kdokoliv, kdo má k vašemu počítači přístup, si je může prohlédnout. Jak se tomu bránit?

OCHRANA DOKUMENTŮ: Chraňte jednotlivé soubory jednoduše hesly pomocí softwaru GnuPG, který jsme již popsali v sekci o šifrování pošty. Libovolný soubor lze jednoduše zašifrovat pomocí aplikace Gpg4win přes kontextové menu Windows. Po instalaci programu stačí na soubor kliknout pravým tlačítkem. Nejprve je ale nutné nástroj v nabídce »GPGee | Configure« nakonfigurovat. Zde musíte například určit cestu k programu („Path of the program“) – zadat cestu k souboru „gpg.exe“ (ten se většinou nachází ve složce „C:\Program Files\GNU)“. Poté je software připraven k použití. Nyní lze pomocí jednoduchého kliknutí pravým tlačítkem šifrovat vybraný soubor či celou složku.

ALTERNATIVNÍ METODA: Zvolte příkaz »GPGee | Encrypt (symmetrical)«. Jakmile vložíte již zmiňovanou „passphrase“, nástroj vaše data zašifruje.

ŠIFROVÁNÍ DISKŮ: Komplexnějším nástrojem vhodným pro šifrování většího objemu dat je TrueCrypt Portable, který najdete na našem DVD. Ten dokáže chránit i přenosná paměťová média. Nyní vám ukážeme, jak lze pomocí tohoto nástroje šifrovat USB.

Rozbalte si program na svém počítači a jeho kompletní složku zkopírujte na USB. Poté program TrueCrypt spusťte a klikněte na »Create volume«. Nyní zvolte možnost umístěnou v horní části nabídky a vytvořte virtuální, zakódovaný disk. V dalším okně vyberte variantu „standardn TrueCrypt volume“ a klikněte na »Next« a poté na »File«. Poté zvolte svůj USB, upřesněte název „kontejneru“, do kterého si přejete ukládat důvěrné informace v kódované formě, a volbu potvrďte pomocí »Save«. Dále určete velikost kontejneru a zadejte „passphrase“.

Nakonec vše potvrďte pomocí příkazu »Format«, který kontejner připraví k použití. Pokud si nepřejete vytvořit další „skrýše“, klikněte na »End«. Váš USB nyní obsahuje šifrovaný datový kontejner, k jehož obsahu se bez programu TrueCrypt a vaší „passphrase“ nikdo nedostane...

Abyste mohli kontejner otevřít a soubor použít, otevřete tento soubor v programu TrueCrypt v nabídce »File | Integrate« a zadejte „heslo“. Poté se v okně „Tento počítač“ objeví virtuální disk s vašimi daty. Pozor: Jakmile jednou uložíte všechny soubory do kontejneru, zavřete je tak, že zvolený „virtuální disk“ označíte a zvolíte příkaz »Disconnect«. Nyní jsou vaše data chráněná, i pokud svůj USB disk ztratíte.

PERMANENTNÍ SMAZÁNÍ: Hrozí-li nebezpečí, že se USB disk dostane do nepovolaných rukou, doporučujeme alternativní opatření. „Nálezce“ totiž může poměrně snadno na disku obnovit i soubory, které jste vymazali. Tomu se nyní můžete bránit například pomocí programu Steganos Shredder, který dokáže data z příslušného média odstranit natrvalo...

AUTOR@CHIP.CZ

Neviditelný plášť: Tento nástroj vám nabídne nejen skrytí adresy...