Anonymita zaručena

Ochranu osobních údajů nebere stát moc vážně. My ano. Chip vám ukáže, jak si na internetu zachovat anonymitu – bez omezení komfortu při surfování. *Andreas Hentschel, autor@chip.cz*

V tomto článku najdete

Obrana proti teroristům, hackerům nebo pirátům – to vše bývá uváděno jako důvod pro špehování na internetu. Ukládají se logy, monitorují se P2P sítě... Zkrátka internetové čmuchání je naprosto běžnou záležitostí. Bezpečnost běžného uživatele internetu však může být touto činností ohrožena. Pokud v budoucnu dojde ke zneužití těchto dat, povalí se na vás ještě více reklamy a spamu – a zvýší se tak riziko různých podvodů. Přitom máte právo na anonymní surfování nebo surfování pod pseudonymem. Pokud tedy provideři a úřady ochranu vašich osobních údajů neberou vážně, musíte si svoji identitu na webu chránit sami. Chip vám ukáže, jak na to.

INTERNET

Cookies & Co.: Účinné maskování identity

Při surfování neustále dostáváte „nálepky“ s vaším ID. To může být nutné z technických důvodů – jako např. u IP adresy. Cookies nebo referrer záznamy však ve většině případů vytváří z čisté zvědavosti provozovatelé webových stránek. Podívejme se tedy na to, jak se těchto zrádných nálepek zbavit.

COOKIES: Vypnout, a přesto pohodlně surfovat – i v IE 7

Díky cookies vědí provozovatelé webových stránek, kdo jste a kam až jste se při svých posledních návštěvách proklikali. Velkorysá základní nastavení všech prohlížečů umožňují ukládání datových paketů, aniž by vás někdo požádal o svolení. Vy však máte možnost toto „doručování nevyžádaných balíků“ zastavit. →

Najdete na ChipDVD **JAP 00.07.001** freeware ■ **TOR 0.1.1.26** freeware ■ **ANts P2P 1.5.8 beta** freeware ■ **Internet Explorer 7 CZ** freeware ■ **Firefox 2 CZ** freeware ■ **Opera 9.10 CZ** freeware

→ **Internet Explorer:** Pokročilým managementem cookies se může pochlubit právě tolik haněný Internet Explorer. Prohlížeč Microsoftu má i v nové verzi 7.0 integrovánu platformu P3P, která v pozadí bdí nad dodržováním pravidel ochrany osobních údajů – a cookies buď připouští, nebo odmítá. Jak to funguje? Platform for Privacy Preferences je platforma standardizovaná konsorciem WWW-Consortium pro výměnu informací o osobních údajích. Každý provozovatel webových stránek, který se P3P účastní, má na svém serveru uloženu dohodu o ochraně osobních údajů, kterou načítá P3P klient integrovaný v IE a porovnává ji s vámi definovanými nároky na zabezpečení. Přes nabídku *Nástroje | Možnosti internetu | Zabezpečení* nastavíte svou individuální úroveň zabezpečení.

Naše doporučení: Změňte standardně nastavenou úroveň zabezpečení „Střední“ na „Vysoká“. Požadavky na ochranu osobních údajů P3P a podrobnější informace o tomto problému najdete na *www.w3.org/p3p*. Pokud se nechcete spoléhat na pravidla Microsoftu, upravte si je sami. Napsat si vlastní osobní pravidla ochrany ale není triviální záležitost. Microsoft na svém vývojovém portálu MSDN (www.msdn.microsoft.com) k tomuto tématu uveřejnil podrobný anglický návod. Na portálu vyhledejte „How to create a customized privacy import file“ (aktivujte volbu vyhledávání „Všechny jazyky“!).

Opera: Otevřete nabídku *Nástroje | Nastavení* a na kartě „Rozšířené“ klikněte na *Cookies*. Pomocí volby „Přijímat pouze cookies navštívených stránek“ zablokujete všechny cookies webových serverů. Pokud máte s ukládáním jakýchkoli dat zásadní problém, vyberte volbu „Nikdy nepřijímat cookies“. Nevýhodou tohoto kompletního odmítnutí je to, že se ve fórech musíte stále znovu přihlašovat. Na některé stránky se dokonce vůbec nedostanete – např. přihlášení na eBay při tomto nastavení nefunguje. Tomu předejdete tak, že přes nabídku „Správa cookies“ povolíte pro konkrétní stránky ukládání cookies. Toto povolení však v našem testu nefungovalo zcela spolehlivě – přihlášení na eBay se i přes povolení nezdařilo. Proto zákaz cookies v případě potřeby dočasně vypínejte. Jde to snadno – stiskněte [F12] a aktivujte volbu *Povolit Cookies*. Při dalším surfování ovšem nezapomeňte blokování znovu aktivovat!

Firefox: Reklamní cookies nejdou bohužel u tohoto prohlížeče jednotlivě zablokovat. Máte na vybranou mezi úplným zablokováním, nebo žádným. Klikněte na *Nástroje | Nastavení* a poté v kartě „Soukromí“ vypněte volbu „Povolit serverům nastavovat cookies“, čímž všechny cookies zakážete. Adresy stránek, jejichž cookies mají být akceptovány, nastavte přes „Výjimky“. Alternativou tohoto striktního přístupu je management cookies, který vám umožní například rozšíření „Remove Cookie(s) for Site“ *(download na https://addons.mozilla.org/firefox/1595/)*. Nainstalujte Add-on, klikněte pravým tlačítkem myši na webovou stránku a zvolte „Remove Cookie(s) for Site“. Tímto způsobem smažete všechny cookies, které otevřená webová stránka uložila.

Referrer: Užvaněný a navíc nepotřebný

Do referreru zapisuje váš prohlížeč informace o použitém operačním systému a nechráněné aplikace (ActiveX, Java atd.). Referrer tak prozrazuje, které webové stránky jste předtím navštívili. Prostředek pro vypnutí referreru nabízí standardně pouze Opera: Otevřete pomocí [F12] rychlá nastavení a odstraňte zatržítko u volby „Zasílat původ (Referrer)“. Pokud chcete při surfování umlčet komunikaci referreru s jinými prohlížeči, budete potřebovat jeden z doplňujících nástrojů, které představíme na následujících řádcích – ty se o to postarají automaticky.

IP ADRESA: Technicky nutná, ale pomocí taktik utajení manipulovatelná

Váš počítač může s jinými počítači na webu komunikovat – posílat e-maily nebo otevírat webové stránky – pouze pomocí IP adresy. Protože provideři internetových služeb v log souborech protokolují, která

NÁSTROJE NA DVD

Všechny anonymizační nástroje z tohoto článku najdete na DVD v sekci Téma měsíce

1 **JAP**
Anonymní surfování přes kaskády „mixů“

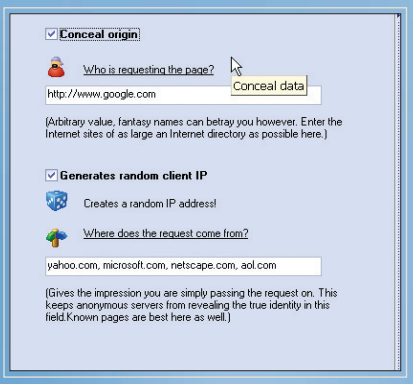
2 **TOR**
Celosvětová anonymizační síť

3 **ANts P2P beta**
Anonymní výměnná burza se šifrováním

Anonymita na netu pro každého

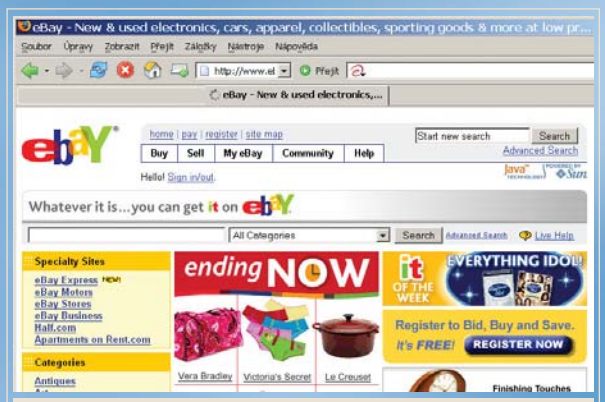
Software z *www.archicrypt.com* kamufluje vaši identitu pomocí anonymizačních proxy, spravuje cookies a mate webové servery.

1 Přes nabídku Actions nastavíte vedle položky *Anonymity* interval pro změnu proxy serverů. Čím je změna častější, tím lepší je výsledná anonymizace – avšak na úkor rychlosti surfování. Kompromisem je hodnota mezi 20 a 30 sekundami



2 Klikněte na nabídku Identita a změňte obsah referreru. Aktivujte položku *Conceal origin* a ArchiCrypt Stealth bude každému cílovému serveru předstírat, že dotaz pochází např. z Googlu – ačkoli jde samozřejmě od vás.

3 ArchiCrypt blokuje známé spywarové komponenty. Tuto ochranu můžete rozšířit: Klikněte pod nabídkou *Spyware* na volbu *Filter all ActiveX components*. Abyste mohli funkci používat, musí být aktivována na hlavní stránce datového filtru.



PROBLÉM ZVANÝ COOKIES: **Pokud máte nastaveno stálé blokování cookies, na některé stránky se nedostanete. Zde např. k přihlášení na eBay.**

→ adresa byla kterému uživateli v danou dobu přidělena, je možné několik měsíců nazpět přesně dohledat, na kterých webových stránkách jste se pohybovali. Doporučujeme vám proto postarat se o ochranu svých osobních údajů sami.

Proxy server: IP adresu je možno utajit tak, že v nastavení browseru nastavíte anonymní proxy server. Takových serverů Google vyplivne na počkání tucty, ale hodný doporučení tento relativně snadný postup určitě není. Datový transfer jde oklikou – a co provozovatel proxy serveru s vašimi daty dělá, to nezjistíte. Lepším způsobem je vsadit na nástroje pro anonymizaci. Ty sice také využívají proxy servery, ale ve většině případů ty důvěryhodné. Spolehlivé jsou open-source projekty Java Anon Proxy (JAP) a The Onion Router (TOR), které najdete na našem DVD. JAP je mimochodem klient projektu AN.ON Univerzity v Řezně a Technické univerzity Drážďany, která je dokonce podporována německým ministerstvem hospodářství – jak protikladný může být přístup dvou sousedních zemí…

AN.ON využívá pro anonymizaci kaskádu minimálně tří serverů Mix-Proxy. To jsou počítače organizací, které provozovatelé JAP označili za důvěryhodné.

Každý „Mix" data pomocí komplikovaného postupu promíchá. Protože jednotliví provozovatelé proxy serverů nejsou spojeni, není na konci možné určit, jaká data si ten který účastník vyžádal. TOR funguje trochu jinak, ale jeho účinnost je podobná. Zde se cesty pro komunikaci generují náhodně z některé sítě vybraného klienta.

Předpokladem pro spolehlivou anonymizaci je u obou postupů velký počet účastníků. Který nástroj použijete, to je na vás. Oba fungují na srovnatelné úrovni zabezpečení. Při našem praktickém testu byla spojení přes JAP trochu rychlejší, ale rychlost kolísá v závislosti na denní době. JAP a TOR se na počítači instalují jako lokální proxy servery. Abyste surfovali anonymně, musíte ještě upravit nastavení spojení, a to následujícím způsobem:

Opera: V nabídce *Nástroje* | *Nastavení* | *Rozšířené* | *Síť* | *Proxy server* zadejte jako adresu »localhost«. JAP použije port 4001, TOR 8118. Důležité: Tyto údaje musíte nastavit také u SSL a FTP spojení.

Firefox: Pod *Nástroje* | *Možnosti* | *Obecné* | *Nastavení* připojení aktivujte volbu *Ruční konfigurace proxy serverů*. Také zde pro všechny protokoly zadejte jako adresu localhost a porty 4001 (JAP), nebo 8118 (TOR).

Internet Explorer: Pod *Nástroje* | *Možnosti internetu* | *Připojení* | *Nastavení místní sítě LAN* aktivujte „Použít pro síť LAN server proxy". Jako adresu zadejte localhost, pro použití JAP port 4001, pro TOR 8118. Potom přejděte na Upřesnit a aktivujte volbu „Pro všechny protokoly používat stejný proxy server".

DOBRÝ MIX: **Čím více uživatelů využívá JAP (v našem případě 987), tím lepší je anonymizace.**

PROHLÍŽEČ: ActiveX musí být vždy vypnuty – jinak zůstanou otevřena zadní vrátka

Ještě jedna důležitá informace: Ve výchozím stavu je většina prohlížečů náchylná na špionáž dat. U Opery a Internet Exploreru vypněte ActiveX (přes *Nástroje* | *Možnosti*). Firefox nemá tuto techniku integrovánu vůbec. Pomocí správných skriptů je totiž možno v prohlížeči spouštět různé procesy – i takové, které provádějí špionáž dat. Sednete-li takovému skriptu na lep, nepomohou ani ty nejlepší triky.

POŠTA

Informace hlavičky: Účinné zametání stop

Anonymní e-mail není žádný problém – vynecháte odesílatele a hotovo. Pokud však chcete vytvořit Usenet-Postings nebo poslat mail na poradenskou službu, aniž byste odhalili své jméno, musíte použít jisté triky.

ŽÁDNÝ ODESÍLATEL: Jednoduché řešení pro příležitostné anonymní maily

E-mailoví klienti nebo webmailery zapíší do hlavičky každé zprávy vaši mailovou nebo IP adresu. Myšlenku přihlásit se na freemailovém serveru (jako je např. email.cz) s nesprávnými osobními údaji raději rychle zavrhněte. Porušili byste všeobecné obchodní podmínky a z toho by mohly být nepříjemnosti. Legálně můžete anonymní maily posílat např. na *www.gilc.org/peech/anonymous/remailer.html*, avšak bez možnosti přijímat odpovědi na své zprávy.

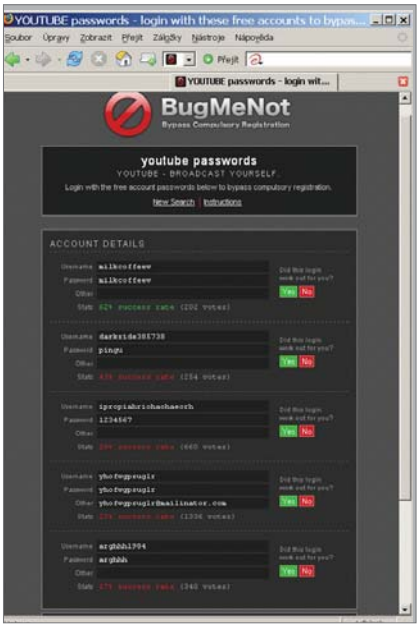
Trvalé anonymní mailování: Bezpečně pouze pomocí Remailer systémů. To jsou e-mailoví klienti s obvyklými funkcemi, kteří z hlavičky mažou odesílatele a všechny další informace, jež by mohly vést k vaší osobě. Takové Remailer systémy jsou řešením spíše pro nadšence, protože jejich ovládání je komplikované. →

→ **Občasné anonymní mailování:** Anonymizátorem mailů pro každého je Hushmail.com, na webu založený freemailer, kde se můžete přihlásit bez zadání svých soukromých údajů. I přes anonymizaci pracuje velmi jednoduše, maily dokonce na přání šifruje pomocí standardu Open-PGP. Bezplatný účet má 2 MB – což není moc, ale pro občasné anonymní maily to stačí. Na placené upgrady, díky kterým máte k dispozici víc paměti, byste však měli raději zapomenout: platí se prostřednictvím kreditní karty – a tím je vaše anonymita směrem k poskytovateli ta tam.

Anonymní pošta

Webová služba Hushmail se snadno ovládá, anonymita je těžko prolomitelná.

Mnoho (především amerických) webových stránek vyžaduje bezplatnou registraci přes e-mail. Pokud svoji e-mailovou adresu nechcete dát k dispozici, a přesto si chcete přečíst článek v New York Times nebo se podívat na zabezpečené video na YouTube, můžete použít následující trik: Na stránce *www.bugmenot.com* se mění data pro přihlášení, a to jak uživatelské jméno, tak i hesla. Na data pro přihlášení příslušné stránky se dostanete jednoduše tak, že do řádku pro vyhledávání zadáte URL požadované webové stránky – a přihlásíte se pomocí daných údajů.

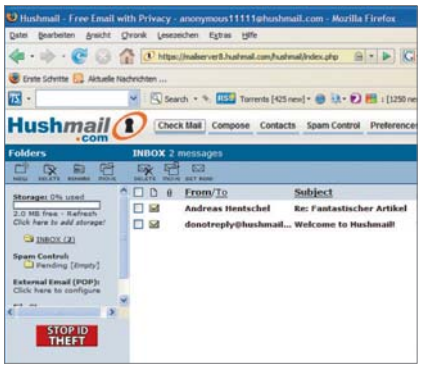


BEZ OBTÍŽÍ: **Snadno a rychle na YouTube – heslo vám poradí BugMeNot.com.**

VÝMĚNA

Sdílení souborů v anonymní síti

Od té doby, co se hudební a filmový průmysl zajímá o uživatele výměnných burz, jsou hlavními podezřelými všichni uživatelé BitTorrentu a spol. – i když jsou výměnné burzy samy o sobě legální. Jedním z možných řešení je sdílení souborů pomocí protokolů nové generace. Ty jsou anonymní a bezpečné.



ANONYMNÍ POŠTA: **Webová služba Hushmail se snadno ovládá, anonymita je těžko prolomitelná.**

ZAŠIFROVANÁ VÝMĚNA: Jak funguje anonymní transfer souborů pomocí ANts P2P

Nové výměnné burzy kombinují decentrální síťovou strukturu BitTorrentu s běžnými anonymizačními technikami jako proxy nebo „mix“. Data jsou přenášena rychle, ovládání je snadné a úroveň zabezpečení vysoká.

Za obzvláště bezpečnou je považována scéna uživatelů sdílejících soubory pod názvem ANts P2P. Klient anonymizuje veškeré datové toky přes vychytralý routing systém. Celý systém funguje jinak než u BitTorrentu, traffic neběží přímo mezi uživateli, ale je přesměrováván přes uzly. Každý účastník zná pouze IP adresu nejbližšího souseda. Odesílatel souboru proto neví, kam je soubor odesílán – stejně tak příjemce neví, odkud soubor pochází.

Další výhodou je skutečnost, že mezi odesílatelem a příjemcem se data šifrují pomocí symetrického Advanced Encryption standardu, takže žádná proxy nebo internetový provider data nemohou sledovat.

Nabídka ANts P2P zatím není tak bohatá jako u BitTorrentu, neustále se však rozšiřuje.

Andreas Hentschel, autor@chip.cz