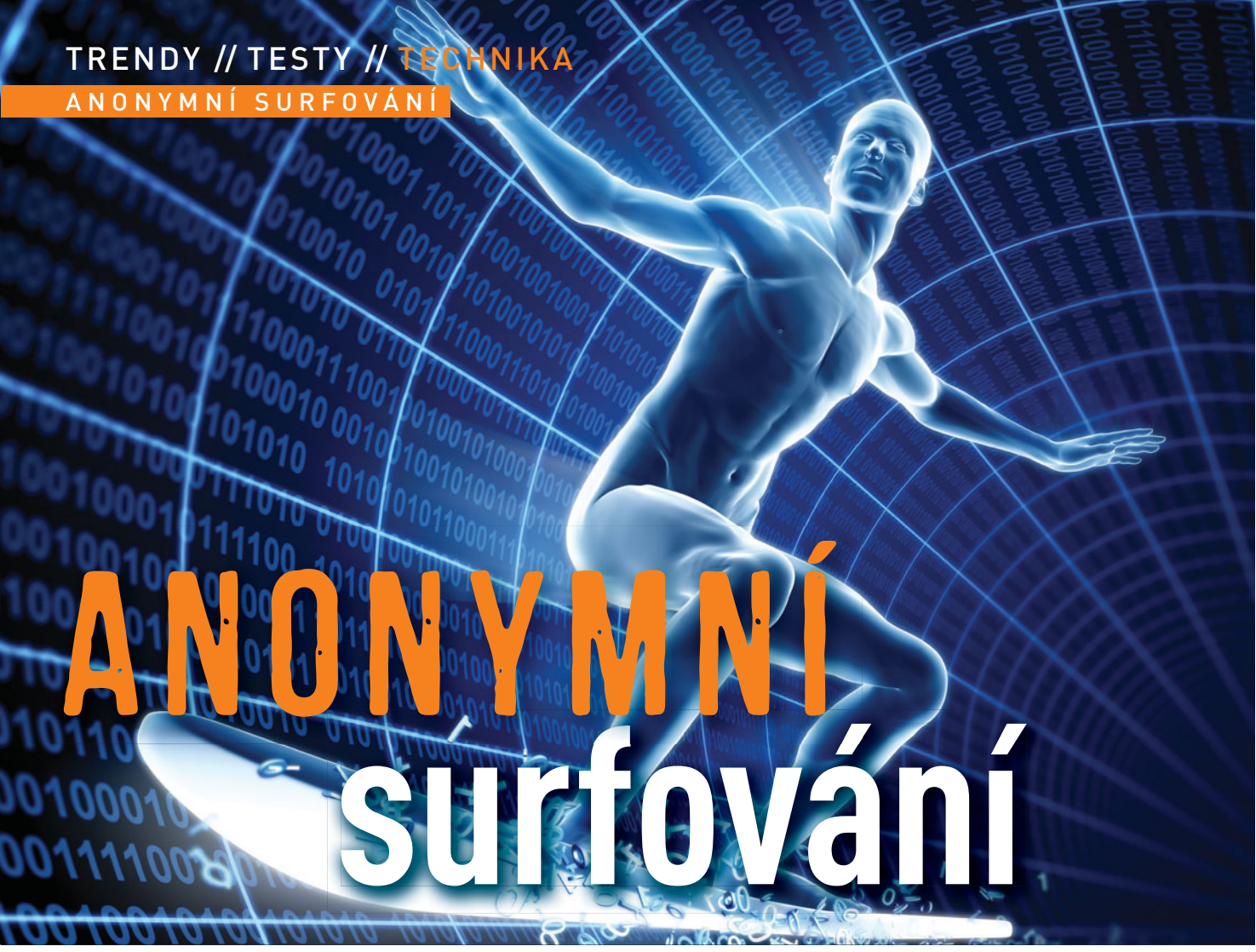


ANONYMNÍ surfování

Soukromí je na internetu čím dál tím nedostatkovějším zbožím. Tisíce subjektů o vás získávají podrobné informace, o kterých nic nevíte a nemáte možnost je ovlivnit. Jsou proto chvíle, kdy se vyplatí být anonymní.

PETR KRATOCHVÍL

V jednom z minulých čísel Chipu jsme vám nabídli exkluzivní pohled do zákulisí reklamních gigantů a jejich honby za informacemi. Vzhledem k tomu, že zisky z internetové reklamy překonávají hranici deseti miliard dolarů, se v žádném případě nedá čekat, že by tyto firmy se špehováním přestaly. Naopak – už při vývoji Internet Exploreru označeného číslem 9 se Microsoft rozhodl do něj integrovat funkci Do Not Track, která umožňuje uživateli prostřednictvím HTTP hlavičky dát webovým stránkám jasný signál, že si nepřeje být sledován (více viz rámeček **na straně 118**). Ve verzi 10 Microsoft nastavil tuto funkci implicitně zapnutou, proti čemuž začala protestovat celá řada reklamních firem a portál Yahoo na rovinu prohlásil, že toto přání uživatelů respektovat nebude. Informace o uživatelích jsou zkrátka příliš cenným zbožím a internetové čmuchaly jen tak něco nezastaví. Je tedy na samotných surfařích, aby si problém vyřešili po svém.

V internetových diskusích o právu na soukromí čas od času zazní, že kdo má čisté svědomí, ten nemá potřebu nic skrývat. Toto pravidlo by jasně platilo v ideální zemi s dobrými zákony a poctivými firmami. V reálném světě plném podvodníků a nepovedených zákonů si každý přemýšlivější člověk musí položit otázku, kam všude mohou doputovat jeho soukromé informace. Pojďme se tedy podívat, jak si lze ochránit své soukromí, aniž by byl uživatel nějak výrazně omezen. Dříve než se pustíme do analýzy možností anonymního surfování, shrneme si, jaké stopy za sebou na internetu zanecháváte. Většina uživatelů ví o IP adrese, host name, případně o použitém prohlížeči a operačním systému. Ve skutečnosti jde o desítky drobných

NA CHIP DVD **Na Chip DVD najdete programy vhodné pro anonymní surfování.**

TOR Anonymizační metoda využívající přesun dat přes anonymní proxy servery. K dispozici je jak oficiální klient, tak portable aplikace využívající Operu.

Jap Program umožňující anonymní surfování díky transferu dat přes skupinu proxy serverů (tzv. kaskád).

Jondo Aplikace využívající stejný základ jako výše uvedený Jap. Bezplatná varianta programu je omezena rychlostí připojení a lze stáhnout soubory pouze do velikosti 2 MB.

CyberGhost VPN Exkluzivní nástroj pro čtenáře Chipu, umožňující anonymní surfování přijatelnou rychlostí. Podrobnější informace najdete na straně 119.

proměnných, ze kterých lze vytvořit téměř identický „otisk prstu“ prohlížeče.

To lze doložit i na webu **panopticlick.eff.org**, kde po kliknutí na tlačítko »Test Me« zjistíte, jak moc je váš prohlížeč unikátní. Dá se očekávat, že většina uživatelů bude nepříjemně překvapena. Pokud se chcete podívat, jaké konkrétní informace lze vyčíst o vašem počítači, navštivte web **analyze.privacy.net**. Některé z těchto informací lze skrýt jednoduše, se zfalšováním jiných budete mít práce mnohem víc. I zde však platí pravidlo, že když se chce, všechno jde.

Anonymně s rizikem

Základní a nejjednodušší cestou k získání alespoň částečné anonymity pro běžného uživatele je použití anonymních režimů v prohlížeči. Ty obvykle zablokují některé identifikační znaky (cookies, Javu, Flash, doplňky), nic ale neudělají s IP adresou. Ta zůstane na navštíveném webu jasně zaznamenaná. Nejjednodušším způsobem, jak ji zamaskovat, je využití webové proxy, kterých je na internetu několik desítek. Mezi nejznámější patří například **www.hidemyass.com**. Nevýhodou tohoto řešení je minimální maskování stop (je skryto pouze několik identifikátorů) a především velké vytížení bezplatných serverů. A komu by se chtělo surfovat (byť anonymně) rychlostí minulého století?

O něco lepší anonymizaci nabízejí klasické proxy servery. I těch je k dispozici celá řada zdarma (viz např. **www.samair.ru/proxy**), trpí ale stejnou slabinou jako jejich weboví příbuzní – nízkou rychlostí. Obě předchozí varianty však mají kromě ubohé rychlosti společnou ještě jednu věc – pro svou anonymizaci využíváte služeb cizích lidí nebo firem a ve většině případů absolutně netušíte, co jsou zač. Nad tím lze mávnout rukou, pokud chcete anonymně přidat příspěvek na diskusní fórum; návštěvu důležitých webů (banky, operátora...) však opravdu doporučit nelze. Před použitím některé ze zmiňovaných služeb lze také navrhnout přečtení jejich podmínek použití, abyste nebyli ve finále nepříjemně překvapeni.

Na závěr je ještě nutné zmínit jeden nepříjemný detail. Nezanedbatelné procento proxy serverů jede na hacknutých počítačích bez vědomí jejich majitelů. Je proto naprosto běžné, že i v aktuálním seznamu serverů jich bude fungovat polovina (majitel nemá zapnutý počítač nebo už hack objevil). Hledání rychlého a stabilního proxy serveru je relativně náročný úkol.

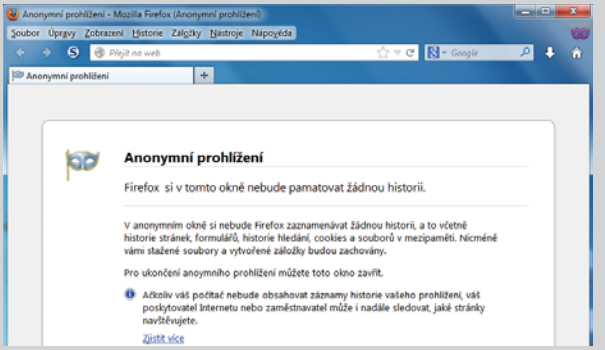
Hide My Ass patří mezi nejznámnější a nejpoužívané webové proxy servery.

ANONYMNÍ REŽIMY V PROHLÍŽEČÍCH

Všechny moderní prohlížeče v současnosti nabízí anonymní režim, který uživateli nabídne alespoň částečné soukromí. Pojďme se podívat, co jednotlivé browsery nabídnou.

FIREFOX

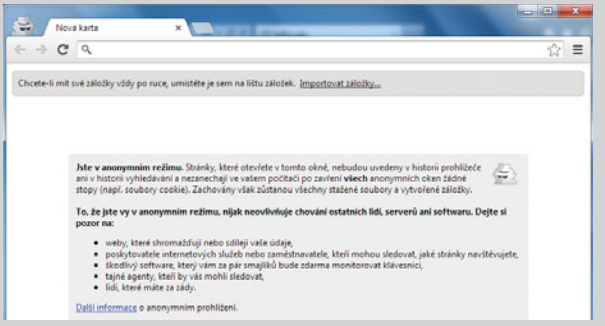
Klávesová zkratka: [CTRL]+[SHIFT]+[P]



Firefox nikdy nepatřil mezi technologické leadery a toto tvrzení jednoznačně platí i pro anonymní režim. V rámci anonymního režimu prohlížeč nezaznamenává žádnou historii, od informací o uložených stránkách přes cookies až po seznam stažených souborů. Podle našeho názoru lze lepší anonymity ve Firefoxu dosáhnout pomocí specializovaných doplňků, které eliminují potenciální stopy.

GOOGLE CHROME

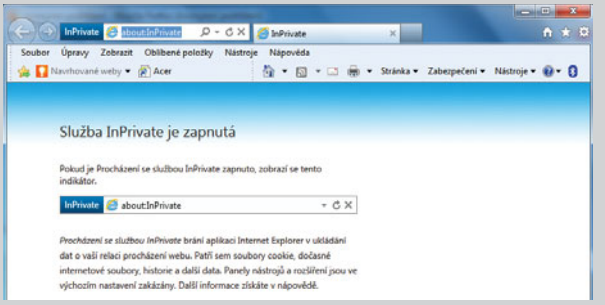
Klávesová zkratka: [CTRL]+[SHIFT]+[N]



Google Chrome nabízí v rámci anonymního režimu podobné funkce jako Firefox – do historie se nezaznamenávají navštívené stránky ani informace o stahovaných souborech. V rámci anonymního režimu se cookies ukládají, po ukončení okna jsou však smazány. Lze jednoznačně prohlásit, že anonymizační funkce v Chrome jsou spíš ubohé – vzhledem k aktivitám Googlu na poli sledování pro reklamní činnost je to i pochopitelné.

INTERNET EXPLORER

Klávesová zkratka: [CTRL]+[SHIFT]+[P]



Anonymní režim je v Internet Exploreru nazýván »Procházení se službou InPrivate«. I přes poměrně bizarní název jde o výkonnou funkci, která je minimálně o třídu lepší než to, co nabízí konkurence. Ani zde se při surfování neukládají citlivé informace (cookies, dočasné internetové soubory, historie...) a je možné zakázat panely nástrojů a rozšíření. Navíc je však obsažena funkce »Ochrana před sledováním«, kterou lze komfortně konfigurovat. Pomocí několika kliknutí ji tak lze například povolit pro správné fungování služby (například u webů Googlu) či zakázat pro přílišnou dotěrnost (Facebook).

ZAJÍMAVÉ WEBY PRO ANONYMNĚJŠÍ SURFOVÁNÍ?

Nabízíme vám přehled těch nejzajímavějších webů, které byste na cestě za anonymitou rozhodně neměli minout

WEBY S ANALÝZOU ANONYMITY
panopticlick.eff.org
analyze.privacy.net

ANONYMNÍ E-MAIL
emkei.cz

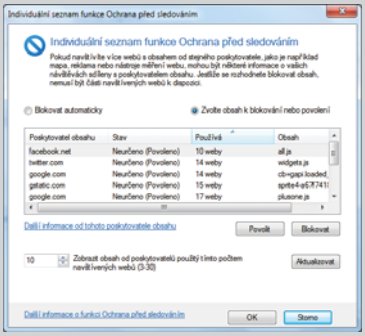
KRÁTKODOBÝ E-MAIL
10minutemail.net/cs
spamavert.com
www.dispostable.com
www.mailinator.com

SEZNAMY WEBOVÝCH PROXY SERVERŮ
proxy.org/cgi_proxies.shtml
www.azproxies.com

SEZNAMY KLASICKÝCH PROXY SERVERŮ
www.publicproxyservers.com/proxy/list1.html
www.samair.ru/proxy
hidemyass.com/proxy-list

VÁLKA KOLEM OCHRANY SOUKROMÍ?

V roce 2007 požádali advokáti skupiny ochrany spotřebitelů Federální obchodní komisi USA (FTC) o přípravu nástroje umožňujícího vytvoření seznamu „Do Not Track" (nesledujte mě) pro on-line reklamu. Tento návrh by požadoval, že on-line inzerenti předají do FTC strojově čitelné seznamy doménových jmen používaných těmito společnostmi, které používají soubory cookie nebo jiné metody pro sledování spotřebitelů. Návrh byl ale smeten ze stolu a poté se téměř dva roky nic nedělo. Až v roce 2009 dva experti z Mozilly upravili myšlenku „Do Not Track" do přijatelnější (pro obchodníky) podoby. Prohlížeče by mohly v rámci http hlavičky požadavku na zobrazení stránky odesílat hlavičku DNT, která webu oznamuje, že uživatel si nepřeje být sledován. Tato myšlenka se ujala a v současné době už funkci „Do Not Track" podporují všechny moderní prohlížeče.



Je ale nutné zdůraznit, že funkce nemůže zákaz sledování vynutit – na straně webů jde o dobrovolnou volbu a dá se předpokládat, že nemalé procento WWW stránek bude tuto prosbu ignorovat. Také ale existují weby a služby (například Twitter), které se chlubí tím, že požadavek uživatele akceptují.

Stojaté vody sledování uživatelů ale nedávno rozvířil Microsoft, když u nově uváděné verze Internet Exploreru s číslovkou 10 implicitně funkci „Do Not Track" zapnul. Kritika především z řad firem žijících z reklamy tvrdila, že o požadavek na vyšší soukromí musí uživatel sám aktivně požádat. Microsoft však svůj postoj obhájil tím, že uživatelé preferují prohlížeč nabízející více soukromí.

Na to poměrně agresivně zareagovala celá řada firem – od úpravy kódu HTTP Serveru Apache tak, aby záměrně ignoroval požadavek „Do Not Track", až po veřejné prohlášení, že bude tento požadavek uživatelů ignorován. V současné době tak lze tuto funkci označit za příjemný doplněk, nikoliv ale za nástroj, který vám zajistí soukromí. O to se musí uživatel postarat pomocí jiných nástrojů.

Za vyšší soukromí

Podstatně vyšší úroveň soukromí (i bezpečnosti) lze zajistit pomocí specializovaných anonymizačních služeb, využívajících kaskádových mix serverů. Ty fungují (zjednodušeně řečeno) jako proxy servery zapojené v řadě za sebou, přičemž konkrétní informaci, odkud a kam proudí data, mají jen dva po sobě následující servery. Data jsou navíc šifrovaná a v rámci sítě také putuje šum paketů znesnadňujících odposlech. V praxi tuto metodu anonymizace využívají sítě JAP a TOR. Teoreticky lze tedy říci, že v těchto sítích je soukromí takřka neprůstřelné, v praxi tomu tak ale zdaleka být nemusí. Podle celé řady zdrojů například v roce 2003 pronikly do sítě JAP německé bezpečnostní orgány a monitorovali komunikaci vybraných uzlů. I přesto lze označit anonymizační postupy za silně nadprůměrné a do karet uživatelům hraje i dobře napsaný software. Například pro síť TOR je k dispozici mobilní verze prohlížeče Opera (s označením OperaTOR), která patří k nejoblíbenějším a nepraktičtějším anonymizačním nástrojům.

Smutnou zprávou na závěr je bohužel to, že ani této metodě se nevyhnula zásadní slabina řešení tohoto typu – příliš nízká rychlost pro každodenní běžné použití. Na diskusní web se tedy bez problémů připojíte, na anonymní stahování balíků dat ale rozhodně zapomeňte.

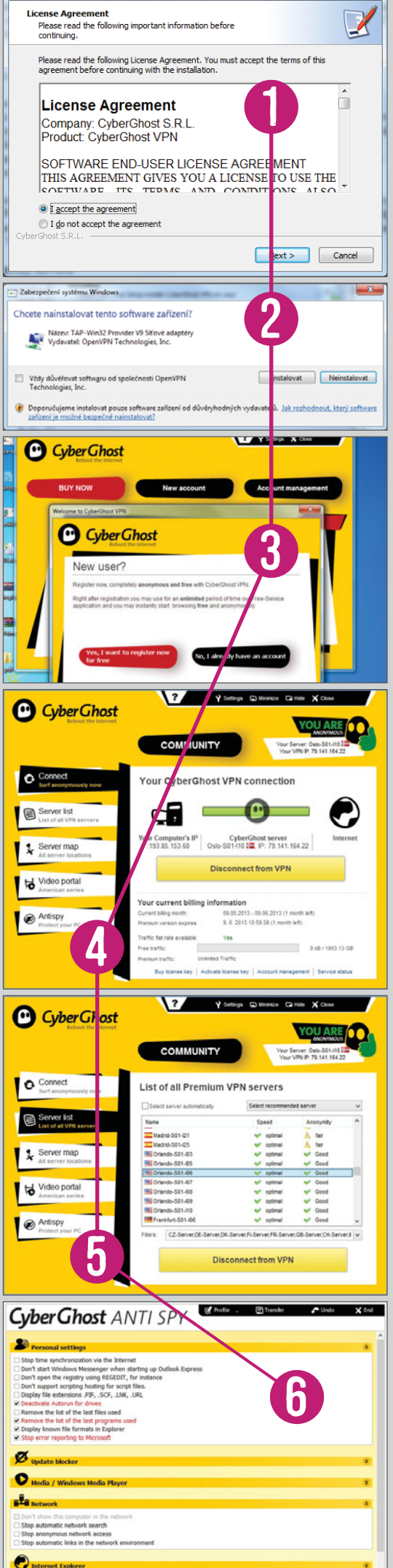
Anonymní pošta?

O anonymním surfování už byly popsány stohy papíru, problém anonymní pošty ale tolik pozornosti nebudí. Přitom však nejde o žádnou drobnost. Obrovské množství internetových služeb vyžaduje kvůli každé drobnosti registraci na e-mail. Pokud pak do formuláře zadáte svůj soukromý e-mail, počítejte s tím, že do týdne bude plný spamu. Řešením tohoto problému jsou tzv. krátkodobé schránky, které fungují jen v řádu minut – což pro registraci zcela postačí.

Jedním z průkopníků této taktiky byla služba 10minutový e-mail (**10minutemail.net/cs**), která se ale stala příliš známou a některé služby už registraci přes ni odmítají. Naštěstí ale existuje celá řada alternativ, které bez problémů fungují, například SpamAvert (**spamavert.com**) – další najdete v rámečku vlevo.

Jiný úhel pohledu na pojem anonymní e-mail nabízí služba na adrese **emkei.cz**. Ta umožňuje odeslání e-mailové zprávy z jakékoliv adresy. Není tak problém si z někoho vystřelit například dopisem z adresy se jménem některé celebrity. Ve skutečnosti samozřejmě e-mail nelze takto snadno zfalšovat. Služba jen využívá nedokonalosti současných e-mailových klientů, které se velmi snadno nechají oklamat – a to platí jak pro Outlook, tak i například pro freemail od Seznamu. Pokud zprávu uložíte na plochu, otevřete ji v jednoduchém textovém editoru (stačí Poznámkový blok) a prohlédnete si hlavičku e-mailu, velmi snadno odhalíte, že jde o podvrh.

PETR.KRATOCHVIL@CHIP.CZ



ANONYMNĚ NA INTERNETU:

Snadněji už to nejde

Na Chip DVD najdete plnou verzi programu CyberGhost VPN ve variantě Premium.

Ta využívá síť proxy serverů k tomu, aby změnila IP adresu a tak vám zajistila anonymitu při surfování po internetu. U programu není limitována ani šířka pásma, tedy maximální dostupná rychlost přenosu dat. Program lze využívat jeden rok od jeho aktivace.

1 PRVNÍM KROKEM JE SPUŠTĚNÍ PROGRAMU, po kterém se objeví okno s možností nastavení jazyka. Čeština zde k dispozici bohužel není, s angličtinou by ale neměli mít problémy ani začátečníci. Poté potvrďte souhlas s licenčním ujednáním a klikněte na tlačítko »Next«.

2 V DALŠÍM KROKU BUDETE VYZVÁNI K POTVRZENÍ nainstalování nového softwarového síťového zařízení. Zde jen klikněte na »Instalovat«. Poté se proklikejte přes instalačního průvodce až do konce.

3 NYNÍ SE OTEVŘE ÚVODNÍ OKNO, kde je nutné se zdarma zaregistrovat. Stačí kliknout na »Yes, I want to register now for free«. V dalším okně pak zadejte zvolené uživatelské jméno a poté dvakrát stejné heslo. Heslo musí mít minimálně pět znaků a musí obsahovat písmena i číslice. Poté potvrďte souhlas s podmínkami použití aplikace a pokračujte tlačítkem »Next«. Program zobrazí váš unikátní PUK kód, který budete potřebovat k případnému resetování hesla ke svému účtu, pokud byste jej zapomněli. PUK kód si můžete vytisknout nebo uložit.

4 POTÉ UŽ SE OBJEVÍ VLASTNÍ OKNO PROGRAMU. Po připojení k VPN můžete vidět, jak se IP adresa vašeho počítače (Your Computer´s IP) při použití programu změní (CyberGhost server). Pomocí názvu uzlu a vlajky můžete identifikovat zemi, přes kterou jste připojeni.

5 POKUD CHCETE ZMĚNIT VPN SERVER, přes který jste připojeni, klikněte na záložku »Server list« a ze seznamu dostupných proxy serverů zvolte ten, který vašim potřebám vyhovuje lépe. Například pro využívání některých amerických služeb (třeba videoserveru **Hulu.com**) musíte využít americký proxy server!

6 DALŠÍ FUNKCÍ PROGRAMU CYBERGHOST VPN je možnost nastavení počítače tak, aby nebylo možné sledovat vaše aktivity: stačí jen kliknout na záložku »Antispy«. V okně, které se zobrazí, najdete možnost deaktivace celé řady služeb. CyberGhost umí například zabránit odesílání zpráv o chybách operačního systému a aplikací Microsoftu, mazat seznamy naposledy použitých programů a otevřených souborů nebo deaktivovat automatické spouštění obsahu pro přenosné disky.