# Totálně pod dohledem:
## 10 tipů, jak se bránit

Na webu už dávno nejste anonymní: každý váš krok v síti potají monitoruje stát i jiné „zvědavé subjekty“. Můžete se však bránit. Ukážeme vám, že lze **SURFOVAT I BEZE „SVĚDKA“**...

MARKUS HERMANNSDORFER

Tvrdíme to odedávna – a nepochybně by nám dal za pravdu i Ústavní soud: tajné špehování bezúhonných občanů je porušováním základního zákona republiky. Jiný názor by asi zastávaly různé státní instituce v čele s ministerstvem vnitra, jejichž snahy o prosazení zákonů poskytujících větší prostor pro sledování obyvatelstva jsou zcela zřejmé. O privátní sféru uživatelů počítačů se však zajímají nejen úřady. Také celý webový průmysl chce co nejpřesněji vědět, na kterých stránkách surfujete a jaké zájmy projevujete – počínaje „informační chobotnicí“ Google a konče nejmenším internetovým obchodem. Na přiloženém Chip DVD vám však nabízíme nástroje, pomocí kterých můžete na internetu brouzdat i telefonovat bez účasti nezvaného „důvěrníka“.

### Obrana před sledováním na internetu ►

**Nástroje: Torpark, JAP/JonDo, JonDoFox**

Své stopy v celosvětové pavučině můžete zahladit surfováním přes „proxy kaskádu“, což je speciální seskupení až několika stovek serverů. Spojení by navíc mělo být silně zašifrováno. To vše vám zaručí buď modifikace browseru Firefox nazvaná Torpark, nebo anonymizační služba JAP.

**TORPARK:** Pro extrahování nástroje na pevný disk nebo USB flash paměť dvojitě klikněte na „zazipovaný“ soubor s příponou ».exe«. Na rozdíl od normálního Firefoxu je Torpark schopen provozu bez instalace.

Pozor, podle posledních zpráv byl projekt Torpark ukončen (verzí 2.0.0.3).

**JAP/JONDO:** Pojmenování služby je trochu záhadné: dokud surfujete prostřednictvím proxy kaskády Technické univerzity v Drážďanech (**anon.inf.tu-dresden.de**), mluví vývojáři o JAP. Pokud v hlavním okně nástroje zvolíte placenou, a tedy rychlejší kaskádu jako »Ramses-Lilie-Jupiter«, jmenuje se nástroj JonDo. Nejsnáze se JAP/JonDo obsluhuje prostřednictvím JonDoFox, modifikované a předkonfigurované verze Firefoxu.

### Obrana před lokalizací mobilů ►

**Nástroj: LocateProtect**

Mobilní telefony jsou sledovány zvláště intenzivně – pomocí falešných základnových


## NAJDETE NA CHIP DVD

### Nejlepší nástroje pro ochranu soukromí

**Torpark** ► bezpečná verze Firefoxu, bohužel vývoj programu byl ukončen

**JAP/JonDo** ► zastírá údaje o vašem prohlížeči

**JonDoFox** ► umožňuje anonymní surfování

**StudiAnalyse (demo)** ► prozrazuje něco o uživateli studiVZ

**TrueCrypt 5** ► šifruje partition Windows

**Zfone Beta** ► šifruje VoIP hovory (SIP)

**CookieCooker (demo)** ► utajuje zvyklosti surfaře

**Proxomitron** ► zastírá informace o browseru

**LocateProtect** ► zabraňuje lokalizaci mobilních telefonů

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

stanic (tzv. „IMSI catcher“), které přístroji předstírají regulérní požadavek od poskytovatele mobilních služeb. Přinejmenším majitelé mobilů s operačním systémem Symbian však tyto tajné požadavky mohou odhalit. Nástroj LocateProtect si nainstalujte pomocí svého softwaru v mobilu, například Nokia PC Suite. Nástroj se spustí samočinně při zapnutí mobilu. Obdrží-li přístroj požadavek od mobilní služby, LocalProtect se zeptá, zda na něj chcete odpovědět – a nechat se tedy lokalizovat. Za normálních okolností odpovězte »Ne«. Pokud však ležíte se zlomenou nohou v ledovcové průrvě, bude nepochybně správnou odpovědí »Ano«. Jen pak vás totiž záchranná služba dokáže najít...

## Obrana před žalobami ►

**Služba: Karaboga**

Také máte chuť všem okolo už jednou od plic říci, co si o nich myslíte? V budoucnu by se vám to nemuselo vyplatit – je jen otázkou času, kdy budou provozovatelé webových stránek, bloggeři a přispěvatelé fór postihováni „za nepřiměřenou či nevhodnou kritiku“ požadavky na náhradu škody a poplatky advokátům.

Například z tohoto důvodu chce „undergroundová“ webová stránka **www.gulli.com**, kriticky zaměřená proti sledování, přesídlit do zahraničí. Přesněji řečeno: chce zamaskovat svůj záznam v databance Whois, v níž jsou uvedeny všechny webové stránky a jejich majitelé. Ublíženci pak při dotazu do databanky už nenajdou adresu Gulli, nýbrž v ideálním případě adresu právníka specializovaného na jednání. Zdá se vám to absurdní a nemožné? Chyba lávky – u nás se podobné případy už několikrát řešily na serverech Lupa.cz a e-komerce.cz...

Díky službě **www.karaboga.net** můžete svou webovou stránku chránit před „obtěžováním“ i vy: služba do databanky Whois zanese nikoli údaje o vás, nýbrž o jistém advokátovi se sídlem v Hongkongu. Anonymizace stojí jednorázově 29 eur. A poněvadž karaboga z ochrany vašich dat žije, hongkongský právník by je vyzradil jen v případě, že byste se dopustili těžkého zločinu.

## Obrana před pátráním po osobách ►

**Nástroje: WebFerret, StudiAnalyse**

Na internetu se nic neztratí. Všechno, co jste mu kdy o sobě prozradili, zůstává někde uloženo – a může tedy být také nalezeno například zvědavým personálním šéfem. Někteří jdou dokonce tak daleko, že kvůli „hříchům mládí“ svých zaměstnanců prohledávají web speciálními nástroji.

Poněvadž nevíte, který vyhledávač pro vaše pronásledování špion použije, musíte nejprve provést „metahledání“, které ukáže nalezené výsledky u všech známých poskytovatelů od Googlu po Yahoo. V případě náruživých surfařů může jít třeba i o 10 000 položek, které je třeba prohledat a vyhodnotit. WebFerret (ke stažení na **www.webferret.com**) se postará o obojí.

Po zadání svého jména do vyhledávacího pole nejprve prostřednictvím »Search Type | Duplicate Removal« odstraňte všechny vícenásobné nálezy. Pak výsledky vyvoláním »View | Arrange Icons« setřiďte. Pokud vám tyto možnosti nestačí, seznam nálezů postupem »File | Save Search« uložte jako soubor ve formátu HTML nebo TXT a pak jej importujte k dalšímu vyhodnocování do Excelu nebo Accessu.

## Obrana před zaznamenáváním rozhovorů ►

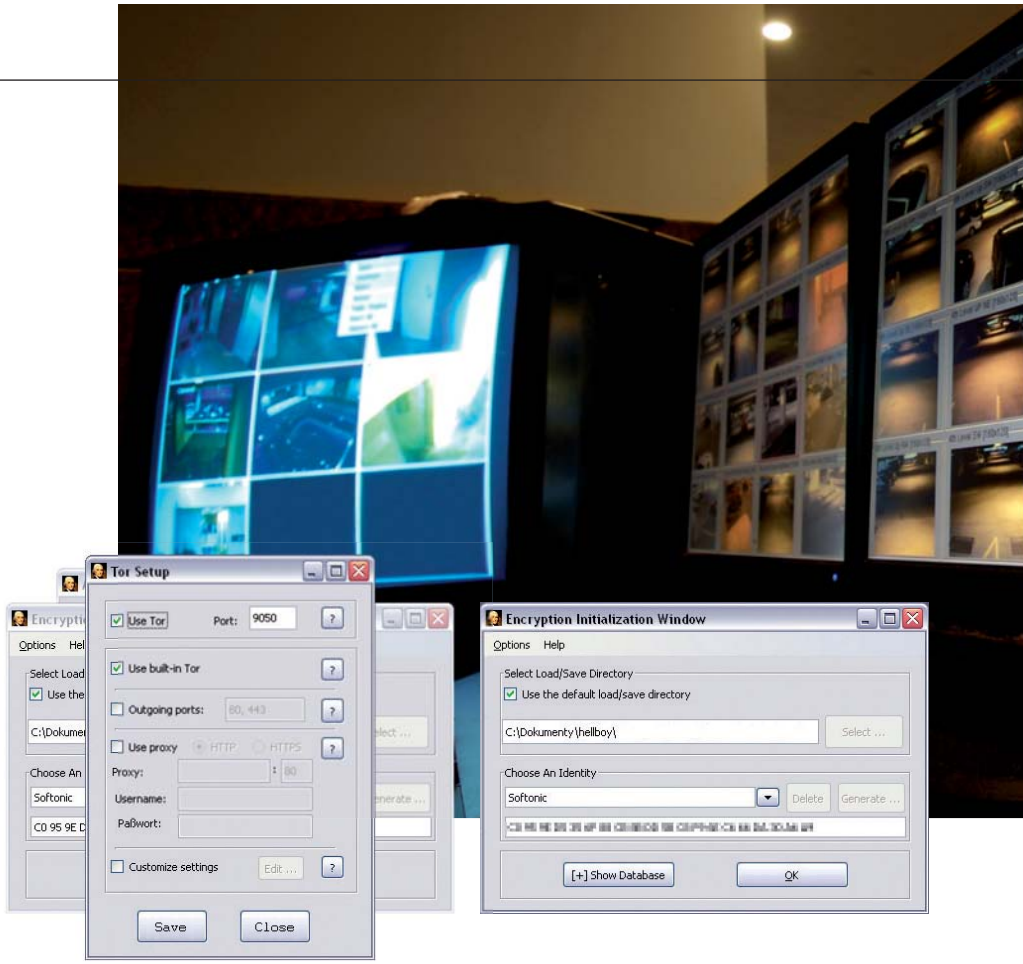
**Nástroje: Scatter Chat, GridIM**

Chatování je čertův vynález, podněcuje osoby s duševními poruchami a mělo by být zakázáno. Zhruba takové mínění mají

různí apoštolové morálky o rychlých komunikačních programech. Abyste i nadále mohli nerušeně komunikovat, své spojení zašifrujte a skryjte svou IP adresu. K cíli vedou dvě cesty.

**CHATOVÁNÍ PŘES TOR:** Scatter Chat (**http://scatterchat.en.softonic.com/**) je založen na instant messengeru a rozhovory šifruje pomocí knihovny libgcrypt a speciálního Scatter Chat modulu. Kvůli utajení IP adresy je obsah rozhovoru veden přes síť Tor.

**P2P ROZHOVOR:** Bohužel teprve v testovacím stadiu je GridIM, k nalezení na **www.grid-evolution.de**. Šifrování u tohoto nástroje je srovnatelné s řešením u Scatter Chat. Pro skrytí IP adresy však tento program používá technologii „peer to peer", známou z výměnných burz. Má tu přednost, že u ní dochází k menšímu zpomalování než u metody využívající Tor. GridIM lze ve formě javaskriptu zapojit do vlastní webové stránky. Jakmile bude k dispozici plná verze, skript přidáme na naši webovou stránku **www.chip.cz**.




**Anonymní chat** Na Gaim založený messenger Scatter Chat šifruje komunikaci a posílá ji po síti Tor. Tak je utajena i IP adresa.

## Obrana před špionáží trojských koní ►

**Tools: TrueCrypt 5.0a, BitLocker (Vista Ultimate)**

Ať už surfujete na internetu, nebo rádi zkoušíte nové programy, k hrozbám, se kterými musíte počítat, patří i desetitisíce špionážních programů a jiných škůdců. Zašifrujte proto svůj pevný disk!

**WINDOWS XP:** Pro XP jsme vám na Chip DVD přidali TrueCrypt 5. Pomocí něj můžete pevný disk zašifrovat na pozadí, zatímco na počítači pracujete. Napříště se vás TrueCrypt krátce před startem Windows bude ptát na heslo (pre-boot authentication). Pro zašifrování systémové partition v nástroji zvolte »System | Encrypt System partition/drive«. V průvodci pak aktivujte »Encrypt the Windows system partition | Single Boot«. Jako šifrovací algoritmus (Encryption Algorithm) doporučujeme »AES-Twofish-Serpent«. Zbytek postupu je jasný.

**VISTA ULTIMATE:** Tato „Windows de luxe" nabízejí v podobě nástroje BitLocker vlastní šifrování jednotek, které si můžete v „uvítacím centru" stáhnout prostřednictvím „Nástroje Vista Ultimate". Je-li váš počítač vybaven TPM čipem (Trusted Platform Module), můžete pevný disk ihned zašifrovat tak, že odpovídající funkci zvolíte po kliknutí pravým tlačítkem myši na ikonu systémového pevného disku. Bez TPM čipu musíte nejprve do vyhledávacího řádku zadat

```
gpedit.msc
```

V okně »Editor objektů zásad skupiny « zvolte »Konfigurace počítače | Šablony pro správu | Součásti systému Windows | Šifrování jednotky pomocí služby Bitlocker «. Nyní v pravé polovině okna dvojitě klikněte na »Nastavení ovládacích panelů: Povolit pokročilé možnosti spouštění« a pak zvolte »Povoleno | Povolit nástroj Bitlocker bez kompatibilního čipu TPM«. Teď zasuňte do portu USB paměť, na niž má být uložen spouštěcí klíč, a ukončete průvodce. Tím je zabezpečena i Vista Ultimate.

## Obrana před odposlechem telefonu ►

**Nástroje: Zfone (Beta), Skype**

Nejdůležitější základní pravidlo pro obranu před odposlechem vašich telefonních hovorů zní: Zapomeňte na pevnou síť. Tady nezmůžete absolutně nic. Protiopatření můžete podniknout jedině v případě internetové telefonie (VoIP). Používáte-li Skype (**www.skype.com**), nemusíte však dělat vůbec nic. Tento poskytovatel šifruje hovory automaticky 256bitovým standardem AES. Funguje to ovšem jen pro telefonáty vedené mezi dvěma klienty Skype.

Máte-li jiného poskytovatele, šifrujte telefonní spojení nástrojem Zfone. Ten se do zná-

## INFO

### Roční historie vašeho surfování

V roce 2005 u nás vstoupil v platnost zákon č. 127/2005, o elektronických komunikacích. Kromě inovací při vymezení některých pojmů a jiného způsobu regulace přináší i další „zajímavé novinky". Například v §97 najdete:

§97 (1) Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna na náklady žadatele zřídit a zabezpečit v určených bodech své sítě rozhraní pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv Policií České republiky.

§97 (3) Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat provozní a lokalizační údaje a tyto údaje je na požádání povinna poskytnout orgánům oprávněným k jejich vyžádání podle zvláštního právního předpisu. Rozsah provozních a lokalizačních údajů, dobu jejich uchovávání, která nesmí být delší než 12 měsíců, a formu a způsob jejich předávání orgánům oprávněným k jejich využívání stanoví prováděcí právní předpis.

Celý zákon si můžete prohlédnout například na **http://zakony-online.cz**.


## INFO

# Nejtrapnější sledovací havárie

Špiclování je špatné, hloupost a ledabylost zde vždy vzbudí škodolibé veselí. Chip prozrazuje, kde a kdy špioni selhali. Nabízíme několik trapasů – bez nároků na úplnost.

### BLAMÁŽ S GOOGLEM

Poněvadž německá extremistická „Militantní skupina“ příležitostně používá slova jako „reprodukce“ a „politická praxe“, pátrači Spolkového kriminálního úřadu zadali tyto pojmy do Googlu. Ihned tak narazili na článek sociologa Andreje H., který tato klíčová slova obsahoval. Tento „důkaz“ úředníkům stačil – H. byl déle než rok sledován a nakonec zatčen. Výsledek akce: 24. 10. 2007 Spolkový soudní dvůr zatykač zrušil kvůli sporným vyšetřovacím metodám.

### POLITIK TERORISTOU

Edward Kennedy, příslušník slavné prezidentské rodiny a jeden z nejznámějších senátorů USA, se nevědomky ocitl na černé listině s popisy podezřelých pasažérů leteckých společností. To mělo za následek odepření letenek a ponižující tělesné prohlídky.

### POŠTĚ SE ZTRÁCEJÍ CÉDÉČKA

Dvě CD, po okraj zaplněná údaji o 25 milionech britských daňových poplatníků, zmizela v roce 2007 během poštovní přepravy. A jako by to nestačilo, přišly britské úřady krátce nato o dalších šest cédéček – byla poslána po stejném kurýrovi, který ztratil už první zásilku. Nedávno jsme se dozvěděli, že už zase chybí další CD, tentokrát s informacemi o DNA několika tisíc osob...

### PROZRAZENÉ TAJEMSTVÍ

Závažné chyby se dopustilo policejní ředitelství ve Friedrichshafenu v září 2007: přísně důvěrné informace se nedopatřením dostaly do rukou veřejného distributora tisku. Úředník podle vlastní výpovědi prostě jen stiskl nesprávný knoflík. Bizarní e-mail obsahoval mimo jiné informace o pátracích metodách Spolkového kriminálního úřadu.

mých VoIP programů typu X-Lite včleňuje jako plug-in. V případě pochybností se zeptejte svého providera, zda jeho software šifrování Zfone podporuje. Také tento nástroj šifruje 256bitovým klíčem AES. Aby vše správně fungovalo, spouštějte nejprve Zfone a až potom VoIP klienta svého poskytovatele.

## Obrana před internetovými profilery ►

**Nástroje: CookieCooker, Proxomitron**

Pomocí cookies a tzv. referrerů dokáží špioni zjistit, kdo jste, které webové stránky jste navštívili a kam jste klikali. Tak si vytvoří váš osobnostní profil, který popisuje vaše zájmy a nákupní zvyklosti. Stačí ale pár triků, a jste pro ně „neviditelní“.

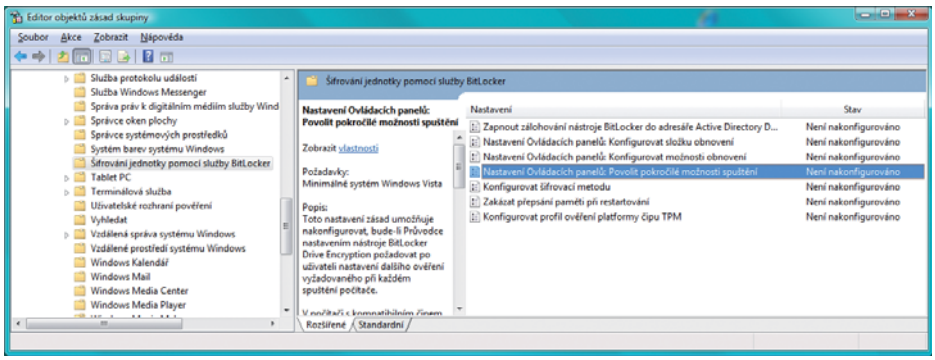
**VYPNUTÍ COOKIES:** V Internet Exploreru nastavte prostřednictvím »Nástroje | Možnosti Internetu | Zabezpečení« posuvník do polohy »Vysoké«, čímž se zbavíte zrádných textových souborů. Pro Firefox jsme na Chip DVD umístili plug-in »Remove Cookie(s) for Site«. Je-li nainstalován, klikněte pravým tlačítkem myši na navštívenou stránku a zvolte »Remove Cookie(s)«. Uživatelé browseru Opera za stejným účelem kliknou na »Tools | Preferences | Advanced | Cookies« a aktivují »Never accept cookies«.

Tyto metody však mají jednu nevýhodu: jestliže váš prohlížeč neakceptuje cookies, na některých webových fórech ap. se musíte pokaždé znovu přihlašovat. Pilní „fóristé“ by proto měli investovat 15 eur do sharewaru CookieCooker. S tímto nástrojem můžete přijímat různé identity, aniž byste přišli o výhody, jako je právě automatické přihlašování. Kromě toho program výborně spolupracuje s nástrojem JAP. Demoverzi najdete na Chip DVD.

**BLOKOVÁNÍ REFERRERŮ:** Těchto informací, které umožňují zpětně vysledovat cestu surfaře po internetu, se zbavíte nástrojem Proxomitron. Po nainstalování programu musíte nejprve provést několik nastavení v browseru. V Internet Exploreru zvolte »Nástroje | Možnosti Internetu | Připojení | Nastavení místní sítě« a aktivujte »Použít pro síť LAN server Proxy«. Jako adresu zadejte »localhost« a jako port »8080«. Pod »Upřesnit« zvolte »Pro všechny protokoly používat stejný server proxy«.

Uživatelé Firefoxu musí pod »Nástroje | Možnosti | Rozšířené | Síť | Nastavení« zvolit »Ruční konfigurace proxy serverů« a i zde zadat adresu »localhost« a port »8080«. Pak už mohou spustit Proxomitron a v klidu surfovat. Nejlépe jsou na tom příznivci Opery: ti Proxomitron nepotřebují a stačí jim prostě klávesou [F12] otevřít „Rychlá nastavení“. Pak zruší zaškrtnutí u »Enable referrer logging«, potvrdí dialog – a už bez obav brouzdají hlubinami internetu.

AUTOR@CHIP.CZ




**Bezpečné:** Vista nabízí nástroje BitLocker pro vlastní šifrování jednotek...