Braňte své soukromí!

V našich končinách platí, že anonymita na internetu je chimérou – pokud je důvod vás dohledat, existují k tomu postupy, a to i když jste na internetu nikdy neuvedli své skutečné jméno.

V ČLÁNKU SE DOZVÍTE:
- kdo a jak může identifikovat uživatele internetu
- jak přistupovat k internetu anonymně
- jak se bránit „odposlouchávání“ dat
- jak ochránit počítač před zvědavci
- jak si na internetu uchovat soukromí

Při jakékoliv internetové aktivitě sděluje váš počítač identifikační údaj: tzv. IP adresu (identifikační číslo), přidělenou poskytovatelem připojení. Internetové služby přitom IP adresu většinou zaznamenávají. Se znalostí IP adresy se poté lze přes záznamy poskytovatele připojení dobrat vašeho jména a adresy – ze smlouvy podepsané při objednání služby nebo třeba menší oklikou přes účet, z něhož za služby platíte. Určitou možností je připojení přes mobil s předplacenou kartou – v tomto případě neexistuje žádná smlouva. Proto také policejní složky chtějí napříč Evropou dlouhodobě dosáhnout zákazu anonymních „předplacenek“.

Ale ani tehdy, máte-li uzavřenu smlouvu, nemusíte propadat paranoii. Existuje totiž zákon na ochranu osobních údajů, kterým se poskytovatelé pod hrozbou tvrdých trestů musí řídit. Výše uvedené platí pro součinnost poskytovatelů s policií. Nemusíte se tedy bát, že by poskytovatelé rozdávali informace o vás a vaší internetové aktivitě komukoliv nebo že by je někde zveřejňovali.

Řadový uživatel nemůže na základě IP adresy zjistit, kdo se za ní skrývá. Může zjistit nanejvýš to, prostřednictvím kterého poskytovatele jste k internetu připojeni a ve kterém městě se nacházíte. Pokud vám ale vadí i to, lze použít anonymizér, což je služba, která při surfování zamaskuje vaši skutečnou IP adresu. Obecně platí, že opodstatněnou potřebu maskovat svou IP adresu řadový uživatel nemá. Nicméně pokud jste jiného názoru, můžeme doporučit anonymizér *www.anonymouse.org*.

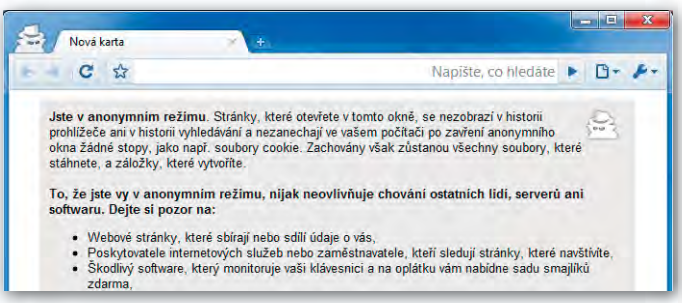
> „V našich končinách nemá řadový uživatel opodstatněnou potřebu maskovat svou IP adresu.“

Anonymizér ale vaši IP adresu zná, takže to není stoprocentní ochrana, jak si třeba myslí někteří nepříliš chytří podvodníčci. O to větší je pak jejich překvapení, když je dopadne policie. Provozovatelé těch seriózních anonymizérů totiž nemají zájem být zázemím pro kriminální živly. Sami by se totiž vystavovali sankcím, takže spolupracují s vyšetřovateli.

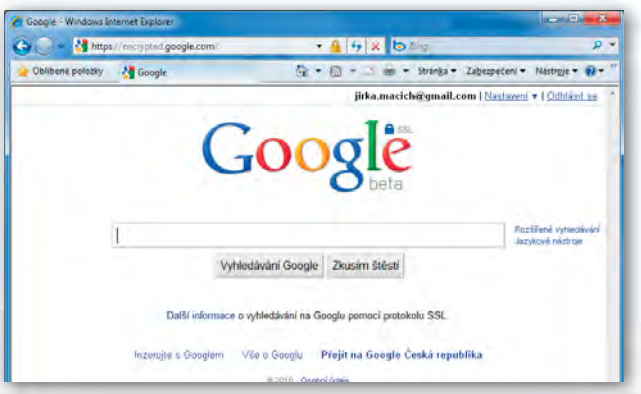
ODPOSLOUCHÁVÁNÍ DAT

Poskytovatel připojení má také možnost sbírat data, která po internetu přenášíte. Teoreticky může sledovat, které webové stránky navštěvujete nebo jaká přístupová hesla používáte k jednotlivým službám. Na to byste měli pamatovat hlavně při surfování přes veřejné bezdrátové sítě. Obranou proti takovému špehování je šifrovaný přenos dat, který zcela běžně používají služby typu internetového bankovnictví. Využívání šifrovaného přístupu se postupně rozšiřuje i na další služby. Dnes je již vcelku běžně poskytováno i pro přístup do e-mailové schránky – alespoň volitelně. To, že komunikace mezi vaším počítačem a webovou stránkou je šifrována, se projeví v řádku s adresou prohlížeče – na začátku adresy vidíte *https://* namísto *http://*. Prohlížeče indikují šifrování různě: např. žlutým podbarvením řádku s adresou nebo zobrazením symbolu zámečku.

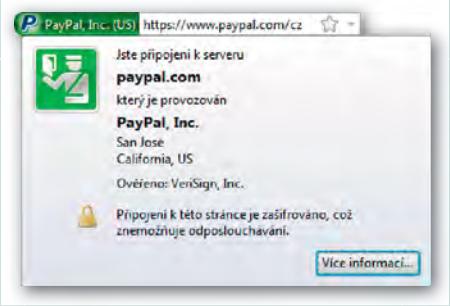
Právě šifrování ochraňuje před odposlechem dat na jejich cestě mezi počítačem a webovou stránkou (službou). Dnes už můžete využít i šifrovaný přístup k vyhledávači. Google nedávno spustil verzi využívající SSL šifrování (*https://encrypted.google.com*). To se může hodit jako ochrana před zvědavým šéfem (v kombinaci s anonymním režimem v prohlížeči) nebo v případě neprověřených veřejných bezdrátových sítí.



Anonymní režim poslouží při surfování na cizím/veřejném počítači.



Už i vyhledávač Google nabízí šifrované spojení.



Šifrované spojení identifikují prohlížeče ikonou zámku.

KOLEGA SLÍDILEM

Velké riziko představuje počítač, pomocí něhož se připojujete k internetu. Webový prohlížeč zaznamenává historii navštívených stránek a volitelně si může pamatovat i přístupová hesla nebo informace zadávané do formulářů. To je velmi praktické, ovšem pouze dokud se k daným informacím nedostane někdo nepovolaný. Proto by měl být počítač řádně zabezpečen i před fyzickým přístupem jiné osoby.

Rozhodně byste neměli opouštět zapnutý počítač, když jste přihlášeni k uživatelskému účtu. Základem je ochrana uživatelského účtu heslem, které třeba kolega v práci nemůže snadno uhodnout. Dále je vhodné nastavit systém tak, aby vyžadoval heslo po deaktivaci spořiče obrazovky nebo třeba po probuzení počítače z režimu spánku / z úsporného režimu. Tak lze zmírnit riziko v situacích, kdy jste se zapomněli sami odhlásit.

Jestliže na počítači pracuje více uživatelů, každý by měl mít svůj vlastní účet s heslem. Tak bude mít každý z uživatelů vlastní uživatelský účet ve webovém prohlížeči a nedostane se k historii navštívených stránek ani k dalším datům jiného uživatele. Pokud pracujete s veřejným počítačem, doporučujeme využít v prohlížeči tzv. anonymní režim/mód (v Internet Exploreru se ukrývá pod názvem InPrivate, v konkurenčních prohlížečích jej naleznete snadno).

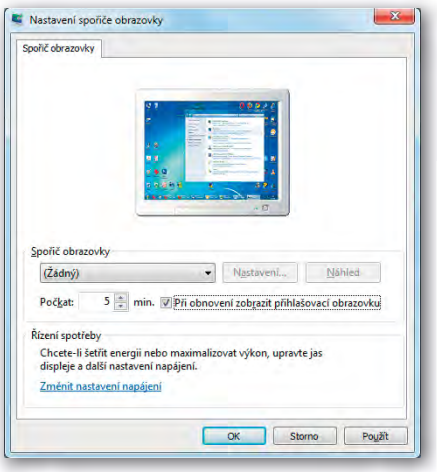
Jeho cílem je, aby na počítači nezůstaly žádné stopy, resp. uložená data. Během surfování buď nejsou ukládána žádná data na pevný disk, nebo se automaticky smažou po zavření prohlížeče (záleží na prohlížeči). Jestliže jste anonymní režim zapomněli spustit, můžete citlivá data smazat i zpětně.

OPATRNĚ S FORMULÁŘI

Nejvíce problémů v oblasti narušení soukromí je s informacemi, které o sobě uživatelé dobrovolně prozrazují. Ještě před pár lety byly největším problémem příliš zvědavé registrační formuláře různých služeb: od e-mailových schránek až po internetové obchody.

I zde samozřejmě funguje zákon na ochranu osobních údajů, ale ne každý jej stoprocentně dodržuje (občas hřeší třeba různé „garážové“ e-shopy), a mnozí uživatelé dokonce dají souhlas k dalšímu nakládání s osobními údaji, takže se tak do značné míry vzdají ochrany ze strany zákona. Kolikrát jste třeba při objednávání zboží na internetu zaškrtli, že souhlasíte se zpracováním osobních údajů dle uvedených podmínek, aniž byste si je skutečně přečetli? Ruku na srdce, alespoň jednou to v životě asi udělal každý (čestným výjimkám tímto vzdáváme hold). Někteří lidé si myslí, že když nejde o vlastnoruční podpis, pak takové odsouhlasení právně nic neznamená.

> „Co se na internetu jednou prozradí, to se už nikdy nemůže se stoprocentní jistotou zase utajit.“



Nutnost zadat heslo po zrušení spořiče uchrání soukromí zapomnětlivých uživatelů.

To je ovšem velký omyl. I na internetu platí, že než něco odsouhlasíte, měli byste si to podrobně přečíst. Do formulářů pak nedoporučujeme zbytečně zadávat informace, které jsou volitelné (které není nutné zadat).

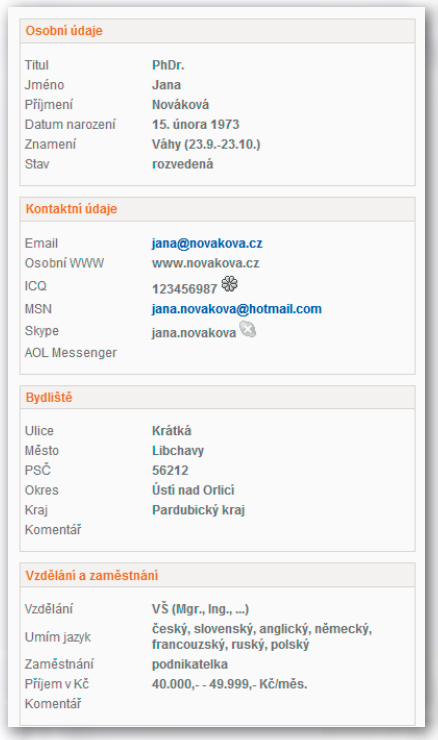
HŘEBÍK DO RAKVE SOUKROMÍ

Zvědavé registrační formuláře už ale opravdu nejsou tím největším problémem. Jsou jím různé komunitní servery a sociální sítě, kde o sobě uživatelé uvádějí řadu velmi osobních informací. Důrazně doporučujeme tyto informace sdělovat s rozmyslem, a to zejména v případech, kdy se zapojujete pod svým občanským jménem. Vždy byste si také měli dopředu podrobně přečíst podmínky užívání daného komunitního serveru, zejména tu část, ve které si obě smluvní strany (vy a provozovatel serveru) vymezují svá práva a povinnosti. Zvýšenou pozornost věnujte hlavně nakládání s osobními údaji.

Dále se pak vždy vyplatí alespoň dvakrát ověřit, s kým zadané informace vlastně sdílíte, resp. kdo je uvidí. Málokdy existuje rozumný důvod, aby vaši skutečnou adresu nebo telefonní číslo viděl náhodný návštěvník vašeho profilu. Proto třeba Facebook a další podobné servery umožňují vybrané informace sdílet jen s přáteli. Ovšem pořád jsou tam tyto informace uloženy, a pokud dojde k narušení bezpečnosti nebo k technickému selhání, může k prozrazení dojít (příklady by se našly).

Obecně platí, že co se na internetu jednou prozradí, to se už nikdy nemůže se stoprocentní jistotou zase utajit, takže při uvádění jakýchkoliv osobních informací – zejména na dnes tolik populárních komunitních serverech – buďte opatrní a sdělení každé informace si raději důkladně promyslete. Položte si vždy otázku: Opravdu to musím uvádět?

Jiří Macich ml., jiri@macich.net



Do internetových profilů není vhodné zadávat vše.