



Znepokojuje vás rostoucí množství spamu ve vaší e-mailové schránce? Představíme vám pomocníky, kteří umí **DOTĚRNÉ SPAMY** odpálkovat.

RADEK KUBEŠ

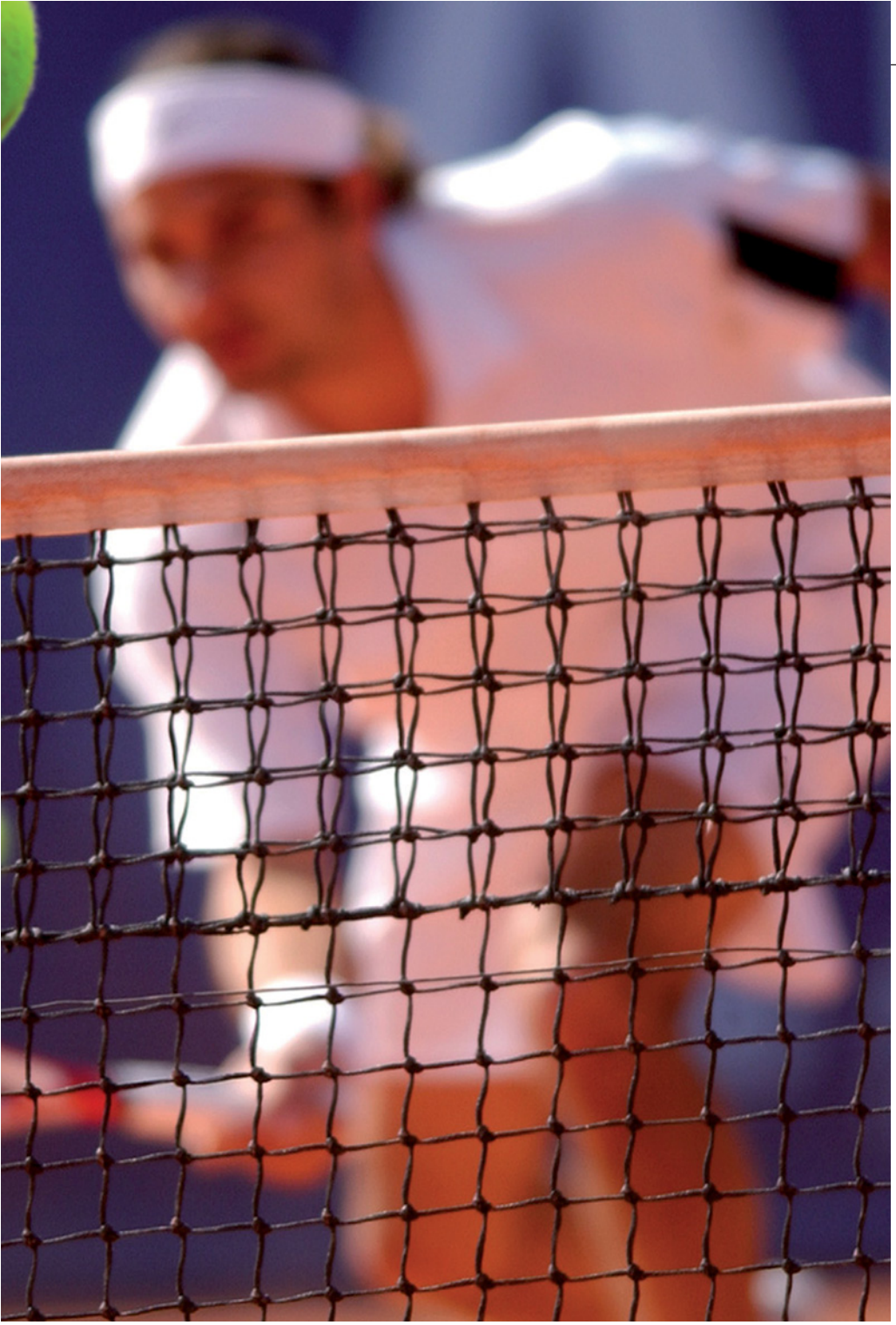
# Pomocníci v nerovném boji

Podíl spamu na celosvětové e-mailové komunikaci se v současné době pohybuje mezi 70 a 80 procenty. Kromě spamu s nabídkami zboží (nejčastěji se jedná o léky, repliky značkových produktů, software, akcie atd.) vám prostřednictvím hromadně rozesílané, nevyžádané pošty hrozí také útoky virů a pokusy o odcizení vašich osobních údajů (phishing). Přestože existují zákony postihující odesílatele nevyžádané elektronické pošty, jsou na stále agresivnější spammery krátké. Jejich útokům je tedy třeba čelit jinými prostředky. Filtry nevyžádané pošty nasazují na své servery provozovatelé freemailů, nechybějí samozřejmě na firemních poštovních serverech a je možné jimi vybavit i váš počítač a používaného e-mailového klienta. Přestože e-mailoví klienti bývají často vybaveni vlastním filtrem nevyžádané pošty, vždy můžete udělat něco navíc – v tomto případě instalací specializovaného nástroje na odhalování spamu. Představíme si nejlepší filtry nevyžádané pošty pro běžně používané e-mailové klienty, které očistí vaši schránku od spamu zcela zdarma.

## MailWasher: Kontrola před převzetím

Princip fungování antispamového programu MailWasher je velmi jednoduchý, a právě proto může tento program spolupracovat téměř s jakýmkoliv e-mailovým klientem a poštovním serverem. MailWasher zkontroluje poštu ještě před jejím stažením do počítače a pomůže vám s identifikací spamu. Teprve po vyčištění schránky na poštovním serveru si do svého e-mailového klienta stáhnete nové zprávy a nebudete si zanášet počítač spamem.

MailWasher startuje po instalaci průvodcem, který buď identifikuje e-mailové účty v Outlooku či jiném e-mailovém klientovi, nebo vám umožní nastavit parametry účtů ručně. Podstatou nastavení je, aby se MailWasher dostal k vaší poště ještě dříve, než si ji stáhne e-mailový klient. Podporován je POP3 i IMAP pro přístup k poště, stačí jen zadat adresu poštovního serveru (zjistíte v nastavení svého účtu na freemai-



## NA DVD

### Nevyžádaná pošta

**MailWasher Free** ► antispam

**SPAMfighter** ► antispam

**Spamihilator CZ** ► antispam

**Spam Terrier** ► antispam

**Plná verze:**
**PC Internet Security 2009** ► ochrana počítače

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

lech typu Seznam, Gmail atp.) a přihlašovací jméno (nejčastěji e-mailová adresa a přístupové heslo). Po výběru nebo ručním nastavení účtu si ještě zvolíte instalovaného e-mailového klienta (z běžně používaných je podporován Outlook, Outlook Express a Windows Live Mail), se kterým bude MailWasher spolupracovat. Tím základní nastavení končí.

Další použití programu je velmi snadné, MailWasher jej navíc demonstruje pomocí krátké animace, přehrávané při spuštění programu. Tlačítkem »Check Mail« zkontrolujete novou poštu na serveru. MailWasher roztřídí poštu na spam, na bezpečné zprávy a na e-maily, u kterých nemůže jednoznačně rozhodnout. Kliknutím na ikon-

## KNOW-HOW

### Techniky boje se spamem

Filtry nevyžádané pošty pracují se dvěma základními technologiemi, založenými na způsobu přenosu spamu po síti a nebo jeho obsahu. Filtrování spamu podle způsobu přenosu je založeno na existenci tzv. blacklistů, greylistů a whitelistů. Blacklisty jsou seznamy e-mailových adres (nejčastěji falešných) a především IP adres, ze kterých bylo zaznamenáno rozesílání nevyžádané pošty. Zprávy ze serverů zařazených na některý z blacklistů jsou antispamovými filtry automaticky odmítány, případně je výskyt odesílatele na blacklistu používán jako jeden z indikátorů při posuzování zprávy spamovým filtrem. Protikladem blacklistů jsou tzv. whitelisty, což jsou pro změnu seznamy bezpečných adres, ze kterých bude pošta bez problému přijímána. V rámci uživatelských nastavení antispamových filtrů si můžete blacklisty i whitelisty doplňovat sami. Pokročilejší alternativou blacklistů jsou tzv. greylisty, které rozhodují na základě stejných vstupních informací (adresa odesílatele), ale přidávají ještě faktor času, konkrétně v podobě dočasného odmítnutí doručení podezřelé zprávy. Spammeři využívající roboty pro rychlé odesílání zpráv na obrovské množství adres se nedoručitelností zpráv zpravidla vůbec nezabývají a ani nezkoušejí nedoručené zprávy opakovaně odeslat. Na svůj útok totiž mají málo času, než je jejich adresa zařazena na některý z blacklistů. Seriózní poštovní servery se oproti tomu pokoušejí zprávu doručit opakovaně a jsou filtry po určité době (řádově desítky minut) odblokovány.

Samostatnou vědeckou disciplínu by mohly tvořit způsoby filtrování nevyžádané pošty podle obsahu. Posouzení obsahu zprávy je totiž velmi individuální záležitostí každého příjemce a nelze jej snadno zobecnit. Filtry založené na pravidlech vyhledávají typické znaky nevyžádané pošty. Může přitom jít o konkrétní slova a slovní spojení (např. viagra atd.), ale i o běžnému uživateli skryté vlastnosti, jako je chybně označený typ zprávy, nekorektní hlavička atd. Filtr přidělí každému indikátoru spamu bodové hodnocení a podle celkového výsledku a nastavené hranice citlivosti je zpráva předána dále, nebo naopak zablokována. Úskalím této metody je především nutnost neustálé aktualizace pravidel filtru v reakci na stále se měnící techniky spammerů. Z tohoto důvodu byly také vyvinuty tzv. bayesovské filtry (podle matematika Bayese), založené na učení se. Inteligentnímu filtru se v režimu učení předkládají zprávy označené jako spam a nespam a filtr si do vlastní databáze ukládá informace charakteristické pro oba druhy elektronické pošty. Filtr pak funguje na základě statistiky a pravděpodobnosti, že zpráva s určitými vlastnostmi je nebo není spam. Bayesovské filtry mohou učit samotní uživatelé ve svých e-mailových klientech (např. Mozilla Thunderbird), nebo mohou fungovat zcela automaticky na poštovních serverech a studovat všechny přicházející e-maily.

## INFO

### Proč se rozesílá spam?

Jistě vás napadne logická otázka, jaký cíl vlastně rozesílatelé spamu sledují, jaký užitek ze zahlcování schránek nevyžádanými zprávami mají. K pochopení smyslu rozesílání spamu s nabídkami na zakoupení léků, softwaru a jakéhokoliv dalšího zboží je třeba si uvědomit, že rozeslání e-mailu na miliony adres téměř nic nestojí. I při zcela zanedbatelné úspěšnosti lze říci, že každá kladná odpověď a pořízení nabízeného zboží jsou pro spammera ziskem. Přesto lze s úspěchem pochybovat o úspěšnosti tohoto obchodního modelu. U nás je známý případ hotelu U Lípy, propagujícího své služby prostřednictvím nevyžádané pošty. Provozovatel hotelu dostal nejdříve od Úřadu na ochranu osobních údajů pokutu ve výši čtvrt milionu korun za rozesílání spamu, a nyní je dokonce v insolvenčním řízení. Ani obrovské množství rozeslaného spamu asi nepřilákalo hotelu nové hosty.

Jinou kategorií jsou spamy slibující úžasné výhry, převody majetku a jiný prospěch za sdělení důležitých osobních údajů (číslo bankovního účtu, kreditní karty atd.). Zde se již točí zajímavé peníze za prodej údajů získaných od důvěřivých příjemců spamu a z vykradených bankovních účtů. Dalším „posláním" nevyžádané pošty je také šíření virů a dalšího škodlivého softwaru, který pak například sleduje aktivitu uživatele a vynáší z počítače citlivá data. V každém případě, neutuchající aktivita spammerů pohání celé odvětví věnující se vývoji technik pro filtrování nevyžádané pošty.

ky označující spam či bezpečnou poštu můžete klasifikaci změnit, MailWasher si přitom vaše rozhodnutí zapamatuje. Kliknutím na tlačítko »Process Mail« spustíte vyčištění pošty a pomocí tlačítka »Mail Program« spustíte svého e-mailového klienta, do kterého si poštu stáhnete a kde s ní můžete dále pracovat. Došlou poštu umí MailWasher samozřejmě kontrolovat i automaticky, podle zadaných intervalů a pravidel. Potřebná nastavení najdete pod tlačítkem »Settings«.

MailWasher používá několik způsobů identifikace a filtrování nevyžádané pošty. Jmenujme především použití blacklistů a whitelistů, filtrování na základě adresy příjemce, použité znakové sady textu, analýzu obsahu nebo učící se filtr, rozhodující na základě klasifikace e-mailů uživatelem. Možnosti nastavení filtrování pošty najdete v okně »Settings« pod nabídkou »Spam Tools«.

Vedle bezplatně použitelné verze Free existuje také placený MailWasher Pro, který umožňuje pracovat s více uživatelskými účty, zobrazuje náhled textu zprávy před jejím stažením z poštovního serveru a neobsahuje reklamní banner. Pro jeden e-mailový účet je ovšem plně použitelná i bezplatná verze.

## SPAMfighter: Neohrožený bojovník

Již během instalace se vás bude SPAMfighter ptát na adresu a heslo k e-mailovému účtu, který chcete očistit od nevyžádané pošty. Následně je třeba vypnout všechny e-mailové klienty v počítači a dokončit instalaci. SPAMfighter přitom integruje své funkce přímo do e-mailového klienta – například Outlooku nebo Thunderbirdu. Po instalaci najdete jeho ovládací prvky v hlavním panelu nástrojů e-mailového klienta. Program komunikuje česky a je velmi snadné jej nastavit a používat. O osudu doručených zpráv rozhodujete pomocí tlačítek »Blokovat« a »Odblokovat«, přímo v prostředí Outlooku nebo jiného e-mailového klienta.

S filtrováním pošty vám pomůže především systém blacklistů a whitelistů a nastavitelná úroveň důkladnosti kontroly příchozích e-mailů. SPAMfighter se zároveň učí z vašich rozhodnutí a sdílí informace pro blokování nevyžádané pošty se všemi dalšími uživateli programu. Funkce SPAMfighteru se neomezují na jeden e-mailový účet, záleží jen na nastavení vašeho e-mailového klienta.

Bezplatná verze funguje v plném modu po dobu 30 dní, poté jsou některé funkce omezeny. Do blacklistu nebo whitelistu můžete například přidat jen 100 adres, přijdete o funkci filtrování pošty podle použitého jazyka zprávy, nemůžete odstranit informační patičku o používání SPAMfighteru z odesílaných e-mailů a musíte se také smířit se zobrazováním reklamy na placenou verzi programu. Bezplatnou verzi SPAMfighteru můžete používat pouze k soukromým účelům. Po zaplacení registrace komerční verze SPAMfighter Pro můžete dále bez omezení využívat všechny funkce antispamového programu – na domácím počítači i v práci.

## Spam Terrier: Roztrhá spam na kusy

Také funkce antispamového filtru Spam Terrier se integrují přímo do poštovního klienta. Během instalace programu je třeba provést bezplatnou registraci a získat licenční klíč. Když dojdete v instalačním průvodci do okna »Free Registration«, ponechte označenou volbu »Get free license now« a do dvou volných řádků zadejte své jméno a e-mailovou adresu. Jakmile kliknete na tlačítko


**Bojovník se spamem:** SPAMfighter se integruje do prostředí Outlooku a podle nastavených pravidel identifikuje nevyžádanou poštu.

»Další«, bude vám v e-mailu odeslán potřebný registrační klíč, který použijete hned v následujícím okně průvodce. Pak už stačí jen dokončit instalaci a spustit e-mailového klienta. Podporován je Outlook v různých verzích, Windows Mail nebo The Bat!.

Po spuštění e-mailového klienta se na hlavním panelu funkcí objeví nové ovládací prvky – tlačítka »Mark as Spam« a »Mark as Not Spam« pro označení spamu a toho, co spamem není. Kromě automatické identifi-


**Zakázaná slova:** Důležitým vodítkem k rozpoznání nevyžádané pošty je také kontrola textového obsahu zpráv, jako to dělá například i Spamihilator.

**SPAMfighter Blacklisty a whitelisty:** Základním prostředkem pro boj s nevyžádanou poštou jsou seznamy povolených a zakázaných odesílatelů zpráv.

kace nevyžádané pošty je klíčovou funkcí programu schopnost naučit se rozpoznávat spam podle vašich preferencí. Průvodce učením spustíte kliknutím na nabídku »Train« v menu »Agnitum Spam Terrier«. V prvním kroku si můžete zvolit, zda budete rozšiřovat stávající znalostní bázi antispamového filtru, nebo zda si začnete tvořit úplně novou. Doporučujeme vám ponechat první volbu a prohlubovat znalosti programu. Dále si vyberte složku, ve které jsou uloženy nevyžádané zprávy, na kterých se má Spam Terrier učit. V Outlooku jde zpravidla o složku »Nevyžádaná pošta«. Následně označte jednu nebo více složek s poštou, kterou nepovažujete za spam. Spam Terrier prozkoumá zprávy ve vybraných složkách a zapamatuje si vlastnosti pošty podle vaší klasifikace na spam a „nespam". Proces učení je samozřejmě vhodné průběžně opakovat a rozšiřovat tak znalosti programu Spam Terrier pro rozpoznávání nevyžádané pošty.

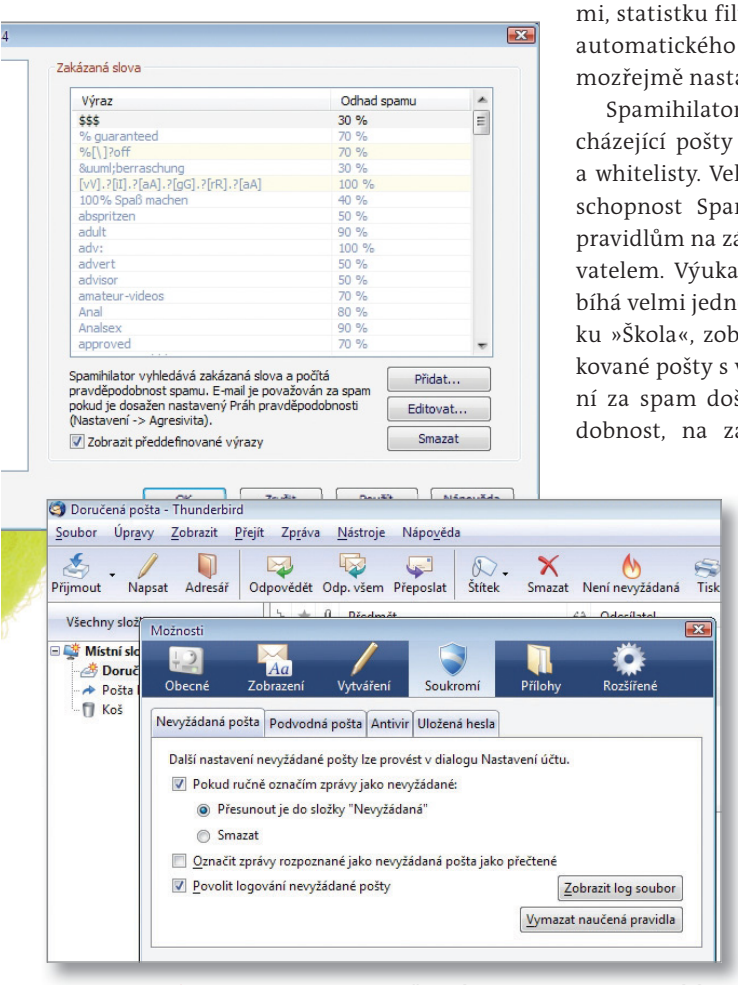
## Spamihilator: Prohlídka na hranicích

Antispamový program Spamihilator sice také spolupracuje s e-mailovými klienty, ale přímo se do nich neintegruje. Výhodou takového přístupu je široká podpora různých e-mailových klientů. Spamihilator pracuje na pozadí operačního systému a o své činnosti dá vědět, pokaždé když e-mailový klient začne stahovat zprávy z poštovního serveru. Spamihilator během stahování zprávy zkontroluje a zablokuje spam.

Instalaci a použití Spamihilatoru zvládne i běžný uživatel. Během instalačního průvodce není třeba měnit žádná nastavení, stačí pouze vybrat používaného e-mailového klienta a označit e-mailové účty, jejichž zprávy bude Spamihilator kontrolovat. Spamihilator podporuje protokoly POP3 a IMAP, prostřednictvím kterých se stahuje pošta do vašeho počítače. Češtinu doinstalujete pomocí jazykového balíčku a uživatelské rozhraní se automaticky přepne při spuštění. Ikona aplikace se usídlí v oznamovací oblasti hlavního panelu Windows (vedle hodin). Po kliknutí pravým tlačítkem myši můžete vybrat zobrazení koše se zablokovanými zprávami, statistku filtrování pošty, funkci učení automatického rozpoznávání spamu a samozřejmě nastavení Spamihilatoru.


Spamihilator používá pro kontrolu přicházející pošty bayesovský filtr, blacklisty a whitelisty. Velmi důležitá je samozřejmě schopnost Spamihilatoru učit se dalším pravidlům na základě klasifikace pošty uživatelem. Výuka rozpoznávání spamu probíhá velmi jednoduše. Pokud zvolíte nabídku »Škola«, zobrazí se vám seznam zablokované pošty s vysvětlením, proč k označení za spam došlo (»Důvod«), a pravděpodobnost, na základě které Spamihilator rozhodl (»Probability«). Pomocí tlačítek »Spam« a »Ne-spam« můžete sami určit klasifikaci zprávy a pak kliknutím na tlačítko »Uč se!« ovlivnit budoucí chování filtru. Další nastavení Spamihilatoru nabízejí například určení priority použitých filtrů (filtr newsletterů, příloh, obrázků, odkazů, zakázaných slov atd.), úrovně ochrany (označeno jako »Agresivita«) a samozřejmě i seznamů blokovaných a povolených odesílatelů zpráv. Možností nastavení je opravdu mnoho, což dává uživatelům značné možnosti při experimentování s optimálním nastavením Spamihilatoru, tak aby propouštěl skutečně jen korektní zprávy a neblokoval jinou než nevyžádanou poštu. Popisky možností nastavení nejsou přeloženy do češtiny ve všech případech, nicméně pro bezproblémovou orientaci v nastavení antispamu bez problému vystačí i méně zkušeným uživatelům.

Velkou výhodou Spamihilatoru je podpora plug-inů, pomocí kterých můžete rozšířit funkce programu při odhalování stále nových druhů nevyžádané nebo nebezpečné pošty.




**Bez další instalace:** Open-source poštovní klient Thunderbird nabízí kromě kompletní nabídky funkcí pro příjem, odesílání, třídění a další zpracování pošty i inteligentní antispamový filtr.

# Spam tvoří až 80 % e-mailů

## Thunderbird: Antispam v základní výbavě

Zatímco Outlook zůstává i v době záplavy nevyžádané pošty nadmíru konzervativní a filtrování spamu se příliš nevěnuje, open-source e-mailový klient Thunderbird obsahuje bayesovský filtr nevyžádané pošty. Thunderbird automaticky posuzuje příchozí poštu a označuje nevyžádané zprávy. Pomocí tlačítka »Nevyžádané« můžete sami ovlivňovat klasifikaci zpráv a doplňovat tak znalosti Thunderbirdu pro filtrování další pošty. Další volby nastavení najdete pod nabídkou »Možnosti« v menu »Nástroje«, na záložce »Soukromí«. Vestavěná antispamová kontrola nicméně vůbec nebrání použití dalších filtrů nevyžádané pošty, které jsme představili.

## Nejlepší filtr?: Pro každého něco

Bezplatně použitelné antispamové filtry z našeho přehledu nabízejí ideální příležitost k experimentování s nastavením kontroly nevyžádané pošty. Antispamovou aplikaci volte především podle počtu e-mailových účtů, jejichž zprávy potřebujete kontrolovat, používaného e-mailového klienta nebo třeba i dostupnosti české verze uživatelského rozhraní programu. Současné použití více filtrů nevyžádané pošty vám ovšem nedoporučujeme. Omezili byste tím především schopnost automatického prohlubování znalostí antispamu na rozpoznávání nevyžádané pošty podle klasifikace obsahu zpráv uživatelem.

RADEK.KUBES@CHIP.CZ