# Chcete čistou poštovní schránku?

Slibují viagru, laciný software a třeba i peníze v hotovosti – přinášejí však jen viry a zlost. Prozradíme vám, jak se lze proti spamovým mailům bránit a reklamní mafii přelstít.

*Andreas Hentschel, autor@chip.cz*

Listopad 2006
**25 816**
**spamových útoků**
za účelem phishingu
Zdroj: Antiphishing.org

Sítě botů na celém světě rozesílají prostřednictvím
**507 000**
**počítačů spam**
Zdroj: ShadowServer.org, stav: leden 2007

**84,5 %**
všech mailů je
**spam**
Zdroj: MessageLabs Intelligence Report, leden 2007

## V tomto článku najdete



Obžalovanému Jeffreymu B. Goodinovi hrozí až 101 let vězení. A to jen proto, že tento 45letý Kalifornan rozesílal hromadné maily, zejména phishingové, jimiž z adresátů podvodně vylákal údaje o jejich bankách a data kreditních karet.

Od té doby, co justice USA aplikuje rigidní antispamové zákony (CAN-SPAM Act), začal spammerům těžší život. I za pouhou propagaci viagry teď hrozí dlouhé tresty odnětí svobody a vysoké peněžní pokuty. Může to potěšit i nás: většina spamu, který dnes a denně ucpává naše mailové schránky, pochází z USA.

### Zbytečný boj?

Zatím však americký boj proti spamovému teroru bohužel zůstává bez zjevného účinku – výskyt spamu v poslední době dokonce ještě vzrostl. Podíl nežádoucích (dnes už bohužel ustálený termín „nevyžádaných“ asi vznikl necitlivým překladem) reklamních mailů na celkovém objemu elektronické pošty leží mezi 90 a 95 %, jak odhaduje René Wienholtz, přednosta výpočetního centra webhostera Strato. „Od podzimu tato hodnota „doslova“ explodovala,“ říká. Ještě v létě se pohybovala mezi 70 a 85 %.

Za strmým nárůstem je třeba hledat vynalézavost spammerů: namísto jednoduchých textových zpráv teď své reklamy šíří prostřednictvím obrazových souborů. Filtry založené na analýze textu zpráv, které až dosud dokázaly poštovní schránku před záplavou spamu spolehlivě ochránit, obrazový spam bez námitek propustí – jeho obsah samozřejmě nemohou rozeznat. Při takto masovém výskytu nepřipadá v úvahu ani nasazení OCR filtrů (Optical Character Recognition, tedy automatické rozpoznávání textu), které spotřebovávají příliš mnoho výpočetního výkonu. Jenom samotné Strato musí denně přefiltrovat zhruba 65 až 90 milionů mailů.

Je-li vaše poštovní schránka zaplevelena spamem, stojí to nejen čas a nervy. Je to navíc i nebezpečné, neboť většina virů se šíří právě cestou e-mailu. Určitě bude tedy lepší vyhlásit spamu válku. Prozradíme vám, jak lze zařídit, aby se vaše mailová adresa vůbec nedostala spammerům do rukou. A pokud vzdor veškeré opatrnosti přece jen nějaký spam dostanete, dozvíte se zde také, jak se takových mailů spolehlivě zbavit.

PREVENCE

## Utajení adresy před spammery

Existuje jedna stoprocentní ochrana před spamem: nikomu neprozraďte svou mailovou adresu. Poněvadž je však taková rada v přímém rozporu se smyslem elektronické komunikace, měli byste se postarat alespoň o to, aby vaše adresa nepadla do rukou spammerů. Existuje několik způsobů, jak minimalizovat riziko, že reklamní mafie vyslídí vaši mailovou adresu na webu.

**Alternativní adresy:** Na mnoha veřejných fórech nemůžete vložit příspěvek bez udání své e-mailové adresy. To samozřejmě vědí i spammeři a seznamy na Usenetu a podobných stránkách neúnavně pročesávají malými automatickými programy, aby tam našli použitelné adresy. Proto pro tyto účely raději používejte jednorázové adresy, jak je například nabízí známá bezplatná webová služba Spamgourmet **(www.spamgourmet.com).**

**Funguje to takto:** Na uvedené stránce jednou zadáte svou korektní e-mailovou adresu a zřídíte si tam fingovanou poštovní schránku. Z ní vám Spamgourmet přepošle nejvýše dvacet došlých zpráv na vaši regulérní adresu – konkrétní počet stanovíte sami. Všechny ostatní maily, které do falešné schránky dorazí, jsou prostě ignorovány. Tak je zajištěno, že například zprávy o odezvách na váš příspěvek ve fóru ještě obdržíte – ale záplavu následujících spamových mailů už ne. Pokud budete později znovu potřebovat takovou „zahazovací“ adresu, jednoduše si zřídíte novou. Je však třeba počítat s jednou nevýhodou: nemusí k vám zaručeně dorazit například ani zprávy od provozovatele fóra.

**Sdílení webových účtů:** Mnohé (především americké) webové stránky vyžadují při vstupu založení bezplatného účtu – pro který musíte zadat svou e-mailovou adresu. Nemáte-li k provozovateli takové stránky důvěru, navštivte BugMeNot.com. Tam si tisíce uživatelů po celém světě sdělují data k takovým účtům – stačí zadat URL stránky, pro kterou potřebujete uživatelské jmé-

## Nejpodlejší spamové triky

**Collateral Spam**
Takové maily jsou záměrně rozesílány na neexistující adresy – v hlavičce těchto zpráv jsou však uvedeny platné adresy zamýšlených obětí spamu. Ty pak obdrží systémovou informaci o neúspěšném doručení – pro filtr nikterak podezřelou – se spamovou zprávou v příloze.

**Good-word Attacke**
Zkušenost učí, že „žádoucí“ maily obvykle obsahují určitá klíčová slova, podle nichž textové filtry zprávy třídí. Toho spammeři využívají a svá sdělení prokládají spoustou takovýchto „dobrých slov“.

**Joe Job**
Pod tímto názvem se skrývají maily s falešným odesílatelem. Cílem útoku je domnělého rozesílatele poškodit – buď obsahem mailu, nebo i výpadkem jeho poštovního serveru vyvolaným přílivem mnoha odpovědí.

**Scam**
Spam může být i zábavný. V epických líčeních jsou popisovány rodinné historky a slibovány provize tomu, kdo pomůže při převodu miliardového dědictví na zahraniční bankovní konto.

**False Positives**
Velký problém představují nezávadné zprávy, které jsou zablokovány příliš „horlivými“ spamovými filtry: zanikají pak bez povšimnutí v přeplněných spamových složkách.

**False Negatives**
Tak se označuje spam, který nebyl jako takový rozpoznán. Dobrým filtrům ho neprokouzne více než dvě procenta – a ta lze s přijatelným úsilím vymazat ručně.

## Špičkové antispamové nástroje na Chip DVD

1 **Mozilla Thunderbird**
Poštovní služba s integrovaným spamovým filtrem

2 **Spamihilator**
Učící se spamový fiiltr

3 **K9**
Bayesův spamový filtr

4 **BugMeNot**
Plug-in pro Firefox umožňující sdílení identit

→ no a heslo. Jak jsme se přesvědčili, například pro populární zpravodajské stránky tento server vždy poskytne platná přístupová data.

Integrujte si BugMeNot jako záložku do Internet Exploreru – jako malý javascript, který umí automaticky provádět jednoduché funkce. Otevřete **www.bugmenot.com** a odkaz „Bugmenot Bookmarklet", který tam najdete v menu na úvodní stránce, zahrňte do svých oblíbených položek v IE. Pak vyvolejte webovou stránku, která po vás požaduje přístupové heslo, a prostě klikněte na tuto záložku. Bookmarklet vám ve vyskakovacím okně nabídne k danému účtu vhodná data, – která pak jen převezmete. Pokud máte aktivován „pop-up blocker", musíte Bookmarkletu při prvním vyvolání povolit otevírání okna.

Ještě komfortněji to jde s Firefoxem. Z našeho Chip DVD si jednoduše nainstalujte rozšíření „BugMeNot". Klikněte pravým tlačítkem myši do pole pro zadávání dat k účtu a zvolte *LogIn With Bugmenot*. Doplněný programek pak vloží příhodné přihlašovací údaje automaticky.

**Skrytí mailových adres na webových stránkách:** Mnozí provozovatelé webových stránek se bezděčně stávají „přispívači" spammerů. Mailové adresy totiž na webu uveřejňují v podobě prostého textu, často dokonce ještě s předřazeným „Mail to:" nebo s přímým odkazem. Běžné triky jako nahrazení znaku @ textem „at" nebo „zavináč" či vložení mezer, které mají slídiče zmást, dnes už téměř žádnou ochranu nepřinášejí – spammeři tyto primitivní lsti dávno znají a své nástroje pro „sklizeň adres" tomu přizpůsobili. A platí to i pro e-mailové adresy uvedené ve formě obrázků. S těmi si lze snadno poradit prostřednictvím OCR (Optical Character Recognition). Účinnější tedy bude vyzrát na spammery jejich vlastními zbraněmi.

Mailová adresa uložená jako obraz: Grafiku ve formátu GIF nebo JPEG můžete učinit „nečitelnou" pro spammery tak, že obrázek obsahující adresu rozdělíte v obrazovém editoru (stačí i Malování) horizontálně na dvě části – zhruba ve vodorovné ose zápisu adresy. Oba dílčí obrázky pak ve svém webovém editoru umístíte tak, aby jejich dělicí linie nebyla opticky rozeznatelná. Tím adresového špiona dokonale obelstíte: obě části obrazu je teď nucen načíst odděleně – ale poloviny písmen už nedokáže doplnit.

Mailová adresa uložená jako HTML text: Na webové stránky zapisujte mailové adresy prostě v kódu HTML – avšak s kamufláží pro zmatení nepřítele. Například namísto „Kontakt: mail@domain.cz" zapište adresu ve svém webovém editoru takto:

```
<P>Kontakt:•<FONT•color=#000000>
mail</FONT>@<FONT•color=#000000>
do</FONT>•<FONT•color=#000000>ma
in.cz</FONT>
```

Kdo se vyzná v jazyce HTML, ihned vidí, že formátování v uvedeném zápisu jsou zcela nesmyslná. Písmu – tak jako tak černému – se v něm neustále přiřazuje barevná hodnota černé (<FONT color= #00000>) a hned se zase deaktivuje (</ FONT>). Automatický „vyzvědač", který načítá zdrojový HTML kód, pak už v takové změti znaků není schopen rozeznat souvislou mailovou adresu. Máte-li chuť, můžete hru dotáhnout až do úplného konce a prostřednictvím HTML „začernit" každý jednotlivý znak adresy.

**No Reply:** Zní to tak jednoduše, že jsme až váhali tento tip vůbec uveřejňovat – evidentně je však stále ještě obsahům spamu věnováno příliš mnoho pozornosti. Pokud tedy obdržíte spamovou zprávu, prostě na ni neodpovídejte. A rozhodně také neklikejte na odkaz, který údajně zajistí vyma- →

## Reklamní mafie: Známí spammeři

**Jméno:** Leo K.
**Země:** Rusko
**Profil:** Rozesílá viry, provozuje sítě botů, šíří farmaceutický a pornografický spam.

**Jméno:** Michael L.
**Země:** USA
**Profil:** Hostuje mnoho spamových serverů, instaluje sítě botů pro rozesílání spamu.

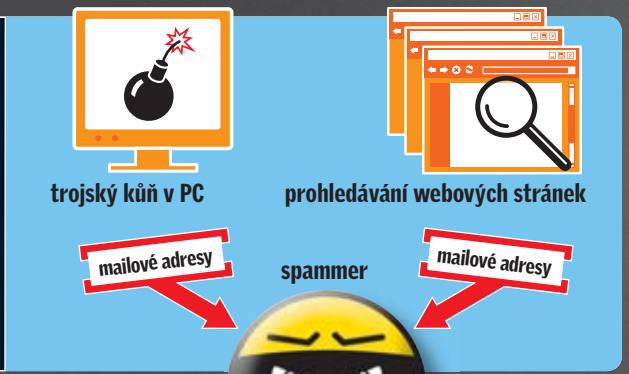
**Jméno:** Alexej P.
**Země:** Německo
**Profil:** Autor „DMS Spamware", který spamuje prostřednictvím sítě botů a otevřené proxy.

Zdroj: www.spamhaus.org

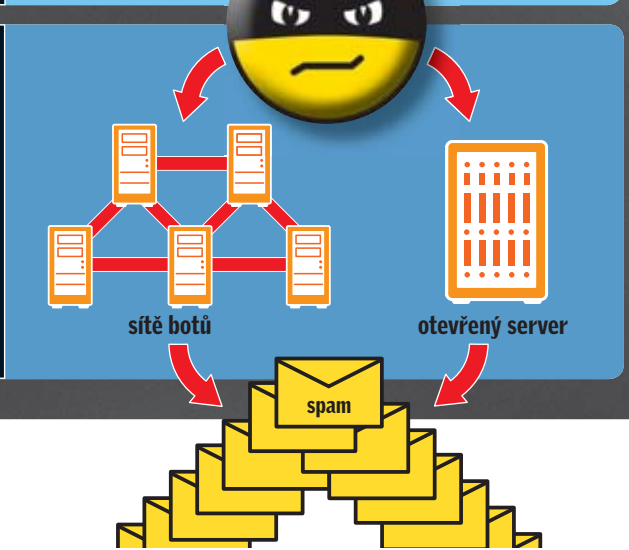
## Jak do PC přichází spam

Spammeři pracují ve dvou krocích: nejprve nashromáždí velké množství mailových adres, načež „zotročí" cizí počítače, které pak jejich reklamy rozesílají.

**1. Sběr adres**
Aby získali co nejvíce mailových adres, používají spammeři programy zvané „address harvester" (neboli něco jako „adresový kombajn"). Anebo ještě drzeji: do cizích PC propašují trojského koně, který jim pak vyzradí všechny uložené kontakty – seznamy adres a příchozí poštu v Outlooku.

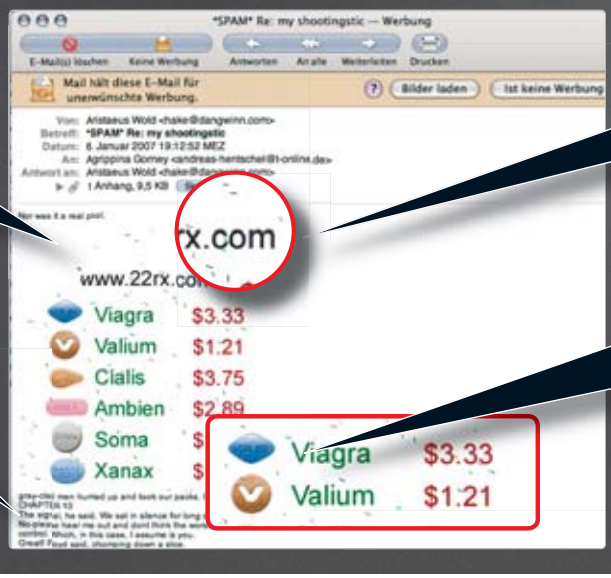



**2. Rozesílání mailů**
Nejčastějšími šiřiteli spamu jsou dnes sítě tzv. botů – zotročených počítačů přinucených „sloužit cizímu uživateli". Každý z nich přitom rozesílá jen malý počet mailů, takže filtrování pomocí „blacklistů" není účinné. Méně častěji se vyskytuje druhá spammerská metoda, která využívá špatně nakonfigurovaných poštovních serverů.



# Nový příval spamu: Na obrazový spam filtry nefungují

Vzdor nasazení filtrů se v mailových schránkách objevuje stále více spamu. Důvodem je skutečnost, že spammeři svá otravná sdělení v poslední době „zabalují" do obrazových souborů. Tímto trikem obelstí filtry, které hromadné maily vytřiďují na základě jejich vždy stejné struktury. Na kontrolní součty obsahu (hašovací hodnoty) se pak už nelze spolehnout.




→ zání vaší adresy z rozesílacího seznamu. Tak totiž spammerovi jenom potvrdíte, že vaše adresa existuje a je aktivní. Výsledkem bude ještě více spamu...

Vyhněte se typickým spamovým adresám: Před nežádoucími zprávami může (alespoň částečně) chránit i správná volba mailové adresy. Máte-li svou mailovou schránku u velkého poskytovatele a vaše jméno se v populaci vyskytuje dosti často, měli byste při volbě mailové adresy projevit trochu fantazie. Takový Josef Novák bude pravděpodobně zaplaven spamem, ať už má mailový účet na serveru Seznam, Volný, Email, či kdekoliv jinde. A nehraje roli ani to, zda má křestní jméno odděleno od příjmení tečkou, čárkou nebo vůbec ne. Spammeři totiž mailové adresy automaticky generují ze seznamů jmen – a stačí jim pak jen trocha štěstí, aby se u Josefa Nováka na doméně Volny.cz trefili do existující adresy.

Pokud máte vlastní doménu, upusťte od obvyklých názvů poštovních schránek, jako jsou webmaster-, admin- nebo info@domain.cz. Spammeři si totiž vytahují seznamy z „Domain Name Serverů" (DNS grabbing) a k takto získaným doménovým jménům pak jen připojují tato často používaná slůvka. A ještě něco: rozhodně si nezřizujte tzv. doménový koš („catch-all" schránku), v němž končí všechny nesprávně adresované maily doručené do domény. Také ten se v krátké době stane jenom sběrnou jímkou na spam.

**Antivirová ochrana**: Obdržíte-li spamovou zprávu, na níž je jako odesílatel uveden váš zná mý (který samozřejmě ani netuší, že by vám něco takového posílal...), pak se v jeho počítači usadil trojský kůň a začal odtud šířit svůj spamový balast. Tady platí jen jedna rada: udržujte svůj antivirový program stále v aktuálním stavu – a poproste všechny partnery, s nimiž si vyměňujete maily, aby učinili totéž.

Během tří měsíců rozeslali dva Korejci

**1,6 bilionu spamových mailů**

Zdroj: Sophos

OBRANA

## Samočinné vytřídění informačního balastu

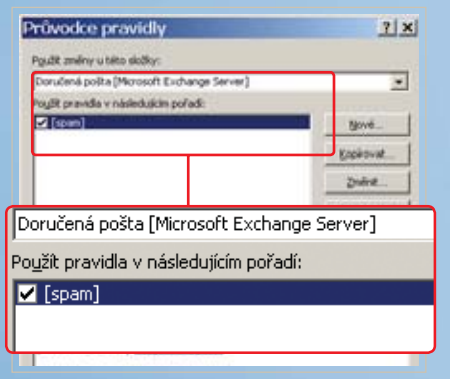
Jakmile se vaše e-mailová adresa jednou ocitne na seznamech spammerů, můžete →

# Využití externího spamového filtru K9 v Outlooku

Spamový filtr K9 můžete nasadit bez nastavování ihned po instalaci. Pro úspěšné potírání spamu však ještě musíte instruovat také svého poštovního klienta. Stačí k tomu několik kliknutí myší:


**1 Přesměrování Outlooku na K9**
Aktivujte *Nástroje | Účty elektronické pošty | Zobrazit* nebo změnit existující účty elektronické pošty a klikněte na *Další*. Zvolte svůj mailový účet a klikněte na *Změnit*. Jako uživatelské jméno zadejte *[váš server příchozí pošty]/110/[vaše uživatelské jméno]*. Pod Informace o serveru změňte server příchozí pošty na *Localhost*.


**2 Úprava nastavení serveru**
V části Další nastavení aktivujte záložku Server pro odchozí poštu. Nyní zaškrtněte položku Server pro odchozí poštu *(SMTP)* požaduje ověřená a pod *Přihlašovat se jako* zadejte své uživatelské údaje. V záložce upřesnit pak u *Čísla portů serveru* vedle *Server příchozí pošty (POP3)* zadejte „9999". Nakonec vše potvrďte.




**3 Přesun spamu do odpadu**
K9 označuje spamové maily příznakem „[Spam]". Pro Outlook proto definujte pravidlo, aby takové zprávy přesouval do složky nevyžádané pošty: Klikněte na *Nástroje | Průvodce pravidly...* a klikněte na *Nové*. Vše ostatní už je jasné: maily, v jejichž předmětu se vyskytuje „[Spam]", automaticky přesouvejte do složky nevyžádané pošty.

→ záplavu mailů už jen tlumit – přímo na poštovním serveru nebo pomocí nástrojů ve svém PC. Minimalizovat spam vám optimálně pomohou následující triky.

**Nastavení pro „junk mail" v Thunderbirdu:** Poštovní klient od Mozilly používá k filtrování nežádoucích zpráv tzv. Bayesových filtrů, které se samy učí. Úspěšnost jejich rozpoznávání je značně vysoká, neboť mohou být „vytrénovány". Filtr je v oblíbeném opensourcovém poštovním programu standardně zapnut, z neznámých důvodů však Thunderbird reklamní „smetí" nepřesouvá automaticky do vlastní složky. Chcete-li takovou složku založit, klikněte na *Tools | Junk Mail Controls*. V záložce Settings zaškrtněte *Move incoming messages as junk mail if the senders is in my address dook* a aktivujte *Junk folder on:*. Jestliže nějaký reklamní mail nebude jako takový rozpoznán, označte tuto zprávu „jako spam" manuálně. Filtr si to pro příště zapamatuje a postupem času se velmi přesně a spolehlivě přizpůsobí. Aby do odpadu byly samočinně přesouvány i maily označené za spam manuálně, aktivujte i tuto volbu v *Junk Filter Settings*.

**Nastavení pro „junk mail" v Outlooku:** Poštovní klient Microsoftu nemá schopnost učení, ale filtruje spam na základě seznamů aktualizovaných vždy při „patchday" Microsoftu – na tom se nic nezměnilo ani ve zbrusu novém Outlooku 2007. Můžete pouze určit, jak „přísně" má filtr třídit. K příslušnému nastavení se dostanete přes *Akce | Nevyžádaná pošta | Možnosti nevyžádané pošty*. Úroveň filtrace je standardně nastavena na hodnotu Nízká, která podle zkušeností zachytí asi 90 % spamových mailů. Lepší účinnost má nastavení filtru na hodnotu Vysoká. Pak se ale občas může stát, že ve spamové složce skončí i zprávy, které byste vyhodit nechtěli – neboli „false positives".

**Externí spamové filtry:** Filtrovací programy jako K9 nebo Spamihilator (oba na Chip DVD) vytřídí nežádoucí maily ještě dříve, než se dostanou do poštovního programu. Tyto nástroje nainstalujete ve svém počítači jako „mail proxy"; nejdůležitější nastavení pro poštovní program Outlook se dozvíte v „bleskovém workshopu" – tipy fungují analogicky i v jiných poštovních klientech. K9 pracuje s Bayesovým filtrem, který je v zaučovací fázi poněkud těžkopádný. Kvůli vytřídění mailů se totiž vždy musíte nejprve pře-pnout do externího programu. Ve Spamihilatoru pracuje kromě učícího se filtru ještě také „spam blocker", který zprávy identifikuje podle jejich kontrolních součtů zaznamenaných ve speciálních databázích – a dokáže tak eliminovat hromadné maily. Na rozdíl od učících se filtrů však mají blokovací programy jednu nevýhodu: jsou závislé na signaturách, jejichž aktualizace vyžaduje zpravidla hodiny, ne-li dny.

**Spamové filtry na serveru:** Všichni velcí poskytovatelé elektronické pošty sami nasazují spamové filtry a ročně investují statisíce eur do jejich dalšího rozvoje. Pokud máte svůj mailový účet u některého z velkých providerů, jste proti reklamním zprávám relativně dobře chráněni – výše uvedené tipy však i pak mohou posloužit jako dobrá doplňková opatření.

*Andreas Hentschel, autor@chip.cz*

Chip dostává **cca 60 000 spamových mailů** každý den