Bannery, pop-up, spam & dialery

Pryč s webovou reklamou!

Vyperte internet dočista: zákeřné dialery, znervózňující vyskakovací okna a obtěžující bannery nemusejí být. Někdy pomůže již pár tajných triků - a dokonce i Windows mají několik osvědčených domácích prostředků proti reklamním skvrnám.

Nová ekonomika strádá a s ní i reklamní průmysl. Kdo se ještě teď pohybuje na trhu s bannery a spol., snaží se tvrdě vystrnadit konkurenci. Formy reklamy a proradné pokusy na internetu tajně založit profily uživatelů jsou stále agresivnější - za takové informace marketingové firmy platí obzvláště dobře, jsou proto velmi žádané. Ochrana údajů je "internetovým šťouralům" zřejmě úplně lhostejná, neboť reklamní servery a špionážní programy bezostyšně sbírají data o:

vašich často navštěvovaných a oblíbených stránkách;
hardwarové konfiguraci vašeho počítače;
vašich nákupech na internetu v posledních měsících;
softwaru nainstalovaném na vašem PC; e-mailových adresách;
vašem bydlišti s kompletní adresou.

Nechcete tyto informace poskytovat? A už vás otravuje webová reklama? Pak si přečtěte tento článek. Zjistíte, jak zastavit vyskakovací okna a bannery, zničit cookies a zablokovat špionážní funkce, protože to všechno stojí přenosovou kapacitu, narušuje to vaše soukromí, nebo dokonce ohrožuje systémovou stabilitu vašeho PC.

V první části tohoto článku se nejprve seznámíte se základními opatřeními, která se dají snadno provést a která obratem ruky odfiltrují nejhrubší reklamní odpad. Druhá část patří specialistům, kteří umějí cíleně vypnout jednotlivé poskytovatele reklamy nebo její formy. Také spam v e-mailech, dialery i bannery v ICQ odstraníte pomocí našich tipů pro jemné vyladění. A nakonec vám Chip ještě představí P3P, nový standard pro ochranu dat na internetu. Abyste hned věděli, jak dobře jednotlivá opatření působí, u každého tipu vám na "speciální liště" ukazujeme, jak jeho pomocí efektivně zabránit reklamě.

Základní čištění

Tipy, které pomohou ihned

Malé, chytré, účinné: Následující tipy a nástroje rychle ochrání vás a váš počítač před vyskakovacími okny, cookies nebo špionážními programy, které se na vašem PC chtějí uhnízdit.

ZNIČTE STOPY PO SURFOVÁNÍ...

Několika hmaty vymažete zrádné informace o svých přístupech na internetové stránky na přání také automaticky. Otevřete nabídku "Nástroje | Možnosti Internetu". Zde nejdříve klikněte na "Dočasné soubory Internetu | Odstranit soubory". Tak se vyprázdní cache, která off-line ukládá webové stránky. Potom klikněte na "Vymazat soubory cookie", abyste odstranili malé hromádky informací, které webové stránky nechávají na vašem disku, protože v těch to je: chrliči reklamy jako Doubleclick vpašují na váš pevný disk cookies, které mohou stále znovu načítat. Jakmile jste si chytili cookie a navštívíte jinou stránku s tímtéž poskytovatelem reklamy, identifikuje vás cookie. Poskytovatel se pak může podívat do své databáze, kde jste již cestovali a na jaké inzeráty jste reagovali. Když už mažete cookies, klikněte hned také na "Vymazat historii", čímž vymažete protokol o vámi navštívených stránkách. Ale co s výrazy, kterými jste nakrmili vyhledávací servery? Rychle pryč s nimi: Zvolte záložku "Obsah", klikněte na "Automatické dokončování" a potom na "Vymazat formuláře". Tím je odstraněn i tento zrádce. Mimochodem, tuto práci lze svěřit programům, které ji za vás vykonají automaticky po každém surfování.

VYMAŽTE SLEDOVACÍ SOUBOR WINDOWS

Soubor INDEX.DAT má pod Windows zvláštní funkci: Internet Explorer v něm ukládá informace o všech dosud přijatých cookies, a to i po několik měsíců. I když tedy odstraníte všechny cookies, zůstanou vaše stopy jako záloha v souboru INDEX.DAT. Hloupé je, že Windows uživateli vehementně zakazují vymazání tohoto souboru. Ale také zde pomůže TIF-Löscher 2.0 - už při bootování. Windows pak pouze vytvoří nový, prázdný soubor INDEX.DAT.

TIP: Opatřete INDEX.DAT alternativně ochranou proti zápisu! K tomu si soubor vyhledejte v adresáři "Documents and Settings\Vaše uživatelské jméno\Cookies".

Klikněte pravým tlačítkem myši na INDEX.DAT a potom levým na "Vlastnosti" a "Jen pro čtení". Uložte toto nastavení stiskem "OK" - přístupy pro zápis z prohlížeče již nebudou možné. Příjemným vedlejším efektem je to, že cookies se pak už ani nedostanou na váš pevný disk. Serveru se však předstírá, že Internet Explorer cookie přijal a uložil. Důležité: Proveďte tento tip teprve tehdy, když je Internet Explorer zavřený a soubor INDEX.DAT byl předtím vyprázdněn pomocí programu TIF-Löscher.

NASAĎTE "POP-UP KILLERY" PROTI REKLAMNÍM OKNŮM

"Pop-up killery" jsou užitečné programy, které se napojí do Internet Exploreru. Poznají, když chce webová stránka otevřít další okno. Odpovídající okno je pak ihned opět zavřeno, dříve než ho uživatel vůbec uvidí.

Problém je ale v tom, že těmto "zabijákům" padne za oběť nejen reklama, ale také užitečná vyskakovací okna. Ta potřebujete například při stahování souborů nebo pro dokončení objednávky v internetovém obchodu. Ještě proradnější však je, že některé webové stránky již používají "detektory pop-up killerů", které hned zablokují kompletní přístup ke stránce, pokud jsou potlačována dodatečná okna. Dejte tedy při použití pop-up killeru pozor na to, aby:

program ukazoval, zda právě blokuje okno;

umožnil na určitých stránkách vyskakovací okna povolit.

Právě tyto schopnosti má nástrojová lišta Google (http://toolbar.google.com). Jakmile zaklepe na dveře vyskakovací okno, Google mu je před nosem zabouchne a hrdě ukáže, kolik duchů reklamního moru už nástroj zastavil.

Pro povolení vyskakovacích oken na určitém serveru klikněte jednoduše na zobrazení "Blokováno", když je stránka zobrazena v prohlížeči. Odpovídající doména bude od té chvíle důsledně z blokovacího nástroje vyjmuta, kdykoli tuto stránku navštívíte. Abyste vyskakovací okno povolili pouze jednorázově, vraťte se po zobrazení "pop-up alarmu" na předchozí stránku a klikněte na odkaz znovu při stisknuté klávese Ctrl.

AD-AWARE ODHALÍ ŠPIONY, DIALERY A REKLAMNÍ PLUG-INY

Provozovatelé reklamy rádi sázejí na spyware. To jsou programy, které na popředí nabízejí (údajně) užitečné funkce, v pozadí však protokolují vaše chování při surfování. Tato data pak slídiče posílají firmám, které z nich vytvářejí uživatelské profily a vyhledávají pro ně vhodnou reklamu. Špionážním programům a jejich poskytovatelům "plivnete do polévky", když svůj počítač pravidelně prohlédnete pomocí Ad-Aware (www.lavasoft.com). Tento pro soukromou potřebu zdarma dostupný nástroj najde také zrádné cookies provozovatelů reklamy, záznamy sledovacího softwaru v registru, dialery i nástrojové lišty bannerů, které se bez optání instalují do IE.

Doporučujeme stáhnout si spolu s Ad-Aware hned také "language pack" a nainstalovat ho. Pak si můžete v "Nastavení" vybrat jako jazyk češtinu. Následně spusťte program, zvolte "Prověřit" a postupujte podle instrukcí. O chvíli později je váš počítač čistý. Udržujte databázi Ad-Aware vždy v aktuálním stavu. Za tím účelem musíte pouze aktivovat připojení k internetu a program spustit. Pak zvolte před každým novým prohledáváním možnost "Hledat aktualizace", aby program aktualizoval svou "databázi škůdců" přes internet.

WEBWASHER VYMAŽE BANNERY DŘÍVE, NEŽ VZNIKNOU

Již dlouho je nástroj Webwasher správnou volbou proti blikajícím reklamním bannerům, ale umí ještě více: blokuje také animované obrázky, které cizímu serveru pro sledování reklamy hlásí, že jste vyvolali určitou internetovou stránku.

Po stažení a instalaci zvolte při prvním spuštění washeru možnost "Bez konfigurace" a již můžete surfovat bez bannerů. Webwasher funguje jako lokální proxy server, který kontroluje všechny stránky, než jsou předány prohlížeči.

Pro dodatečná nastavení klikněte vpravo dole na nástrojové liště na symbol "W". V možnostech se pak dají podmínky filtru zostřit tak, že na vašem PC již neskončí ani žádná vyskakovací okna nebo cookies. Kromě toho může nástroj na přání odfiltrovat také obrázky, nebo dokonce multimediální obsahy jako integrované videosekvence. To nejlepší na Webwasheru: pro soukromé uživatele je zdarma. Najdete ho na www.webwasher.com.

Pomocí několika hmatů oddělíte svůj PC od reklamy, spamu a útoků dialerů. Následující tipy ukáží, jak na to - triky propagátorů jednoduše použijete proti nim.

PŘESMĚRUJTE SOUBOR HOSTS

Na každém počítači s Windows existuje malý soubor jménem HOSTS. Používá se především pro přiřazení jmen počítačů v lokálních sítích. Přesněji - funguje jako určitý druh "adresáře", když uživatel zadá webovou adresu. Pokud Windows tuto adresu najdou v souboru Hosts, načte se stránka HTML z lokální sítě, jinak se dotaz přesměruje do internetu. Takzvané "bannerové firmy" rády zneužívají soubor Hosts, aby přesměrovaly dotazy na své inzertní zákazníky - tato metoda se však dá stejně tak dobře použít proti reklamním trikařům. Za tímto účelem jednoduše přesměrujte doménová jména známých poskytovatelů inzerce na lokální proxy server Windows, který má vždy adresu 127.0.0.1.

Jednoduše to vyzkoušejte: Otevřete v Poznámkovém bloku tento soubor z adresáře SYSTEM32\ DRIVERS\ETC, umístěného v adresáři Windows (u Windows 98 je tento soubor hned v hlavním adresáři). Zapište nyní dolů řádek "127.0.0.1 ad.doubleclick.net" (bez uvozovek) a uložte soubor Hosts - bez přípony souboru! Potom navštivte www.ebay.de a podívejte se na pár nabídek. Místo bannerů tam vidíte jen prázdné okno s poznámkou "Akce přerušena". Není divu, neboť prohlížeč kvůli záznamu v souboru Hosts považuje váš počítač za "ad.doubleclick.net" a na vašem počítači banner samozřejmě není k nalezení. Mimochodem, pokud na vašem počítači běží webový server, objeví se místo "Akce přerušena" chybové hlášení serveru - většinou "Error 404" nebo "not found". Tímto postupem můžete vypnout stovky inzertních serverů, aniž byste museli instalovat dodatečný software jako Webwasher, který reklamní odpad a některé jiné požírače šířky pásma též odstraňuje přes interní proxy 127.0.0.1.

Pokud se vám ruční zadávání mnoha reklamních serverů zdá příliš pracné, můžete sáhnout také po předkonfigurovaných souborech Hosts. Asi nejrozsáhlejší soubor Hosts s několika stovkami záznamů najdete na webu na adrese http://accsnet.com/hosts/get_hosts.html. Stáhněte si aktuální verzi předkonfigurovaného souboru a zkopírujte ji do adresáře C:\WINDOWS\SYSTEM32\DRIVERS\ETC ve Windows XP, případně u Windows 98 do hlavního adresáře Windows - a na trhu inzerce je klid. Čas od času se podívejte, jestli existuje nová verze souboru Hosts - je stále rozšiřována.

ZASTAVTE SPAM INFORMAČNÍ SLUŽBY WINDOWS

Sedíte u počítače, surfujete, najednou se na pracovní ploše objeví varování: "Našli jsme na vašem PC bezpečnostní mezeru...". A aby starost o vaši bezpečnost byla dokonalá, najdete na udané webové stránce ihned také program pro zaplnění bezpečnostní mezery.

Neskočte na takový "pop-up spam". Vyskakovací okno pochází z informační služby Windows, která na portu 135 čeká na příchozí zprávy. Tento systém byl vlastně vytvořen, aby síťoví administrátoři mohli svým klientům vykouzlit důležitá hlášení přímo na obrazovku, ale také aby si rozesilatelé reklamního spamu rychle všimli, jaké možnosti jsou s tím spojeny.

Abyste takovému spamu zabránili, nejlépe službu Windows Messaging úplně vypněte. Ve Windows XP se tak dá učinit přes "Ovládací panely | Výkon a údržba | Správa | Služby". Tam dvakrát klikněte na informační službu, zvolte jako typ spuštění z "Deaktivováno" a klikněte na "Ukončit", abyste službu vypnuli. Od této chvíle máte klid od pop-up spamu.

Uživatelé Windows 98/Me by se naproti tomu měli podívat přes "Ovládací panely | Sítě" na záložce konfigurace, zda je aktivována položka "Uvolnění souborů a tiskáren pro sítě Microsoft". Pokud nepoužíváte žádné síťové funkce, můžete také zde tuto službu klidně vypnout, abyste spamovým zprávám na své pracovní ploše jednou provždy zamezili.

JAK SE ZBAVÍTE "POCHODUJÍCÍ REKLAMY BEZ OKNA"

Reklama se stále častěji objevuje ve formě animací Flash. Ty blikají, skáčou po obrazovce a jsou sotva kontrolovatelné. Jednou běhají reklamní figurky přes text, jednou se skládají i celé bannery výhradně z animací průmysl tak chce obranná opatření uživatelů proti nesnášeným bannerům a vyskakovacím oknům přelstít.

Abyste přesto mohli nerušeně surfovat, sáhněte po radikálním opatřením: přejmenujte adresář, ve kterém je uložen plug-in Flash. Najdete ho v C:\WINDOWS\SYSTEM32\ MACROMED\FLASH. Překřtěte ho například na "FLASHX" - na shledanou, nesnášená reklamo! Pokud se přejmenování nepodaří, Flash se právě používá. V tom případě zavřete všechna okna Internet Exploreru a zkuste to znovu.

Výhoda oproti smazání plug-inu: Pokud přece jen narazíte na stránku s potřebou Flashe, což se často stává obzvláště na stránkách o filmech, dáte adresáři jednoduše zase jeho staré jméno a užijete si plný zážitek z Flashe. Tento postup má bohužel jednu nevýhodu - zůstává manuální prací.

RADIKÁLNÍ ANTISPAMOVÁ OCHRANA PRO ACTIVEX

Od té doby, co existuje ActiveX, způsobuje toto proprietární rozšíření prohlížeče od Microsoftu pravidelně starosti. Přes ActiveX se tlačí stále více virů nebo reklamy na pevný disk. Dokonce dialery se instalují jako ActiveX-Control na pevný disk. Toto riziko nemusíte podstupovat. Jednejte proto radikálně: vypněte ActiveX! V Internet Exploreru to jde nejrychleji přes "Nastavení | Možnosti Internetu | Bezpečnost". Zde nastavte "Bezpečnostní zónu" pro internet na vysokou bezpečnost. Tím je ActiveX vyřízený. Pak ovšem zastaví svou práci také Java a JavaScript. Abyste tomu zabránili, přepněte bezpečnostní zónu na střední hodnotu a klikněte na "Přizpůsobení stupně". Potom v části "Řídicí elementy ActiveX a plug-iny" nastavte všechny možnosti na "Deaktivovat". Výsledek: ActiveX je vypnutý, Java se však dá bez problémů dále používat.

VYPNĚTE REKLAMNÍ ANIMACE JAVASCRIPT

Znervózňuje vás nějaká stránka s poskakujícími animacemi, které sledují ukazatel myši? Nebo tato grafika, která překrývá text, jednoduše nechce zmizet? Pak máte co do činění s dynamickým HTML. To sice dobře vypadá, většinou ale jen zatěžuje. Abyste tento druh reklamy jednou provždy zakázali, vypněte JavaScript. Za tím účelem se znovu obtěžujte v Internet Exploreru do nabídky "Nastavení | Možnosti Internetu | Bezpečnost" a pod "Přizpůsobením stupně" vypněte možnost "Active Scripting". Nevýhody jsou ovšem značné: mnoho stránek bez JavaScriptu nefunguje správně; nabídky pull-down nelze vyvolat nebo chybějí textové stránky.

VYPNĚTE JAVA APPLETY - MÉNĚ LEGRACE, ALE TAKÉ MÉNĚ STRESU

Java sama o sobě není považována za obzvláště nebezpečnou, jelikož kód Java běží v chráněném "sandboxu", který nemůže ohrozit zbytek systému. Ale tato bezpečnost nechrání před nadbytečnými reklamními applety, které kradou šířku pásma. Pro vypnutí Javy můžete v Internet Exploreru nastavit bezpečnostní zónu na "vysokou", jak bylo popsáno v předchozím tipu. Nebo necháte bezpečnost na "střední" a vypnete v "Přizpůsobení stupně" všechny možnosti pro Javu.

ZAMČENO: TAK OPATŘÍTE JEDNOTLIVÉ STRÁNKY OMEZENÍMI

Byli jste na některé stránce téměř bombardováni vyskakovacími okny, skrytými dialery a hromadami bannerů? Nechcete se ale vzdát informací za tou záplavou inzerce? Potom uložte URL stránky do "omezených serverů" Internet Exploreru. Ty najdete v nabídce "Nastavení | Možnosti Internetu | Bezpečnost". Zde klikněte na "Omezené servery" a zapište jméno domény.

Pro tento druh internetových serverů by měl být nastaven bezpečnostní stupeň "Vysoká bezpečnost". Potom nehrozí při příštím vyvolání žádné nebezpečí od dotčeného serveru, neboť ActiveX, Java, Active Scripting (a tím také JavaScript) jsou vypnuté a to jen explicitně pro tuto webovou stránku. Po zapsání do "Omezených serverů" například již není možné, aby poskytovatel nastavil svou vlastní adresu jako výchozí stránku pro Internet Explorer.

Kromě toho Explorer také ignoruje tag meta-refresh, který přiměje váš prohlížeč, aby načetl jinou stránku než původně zvolenou - velmi oblíbená hra ušmudlaných a crackerských stránek.

Tento proces můžete také automatizovat. K tomu si pomůžete záplatou registru jménem "IESPY-AD", která na vás čeká na adrese www.staff.uiuc.edu/~ehowes/resource.htm.

Stáhněte z této webové stránky soubor zip a rozbalte ho. Po dvojím kliknutí na dávkový soubor INSTALL.BAT uvidíte instalační nabídku. Tady zvolte možnost "2". Tím bude po bezpečnostním dotazu opatřen dlouhý seznam webových serverů nejvyšším stupněm bezpečnosti v IE. Tyto servery jsou obzvláště známé pro "Ad-Spamming" - jen se to tam hemží dialery a nesčetnými vyskakovacími okny. Potom bude váš Internet Explorer surfovat zase o něco bezpečněji. Inzerci samotnou tato záplata samozřejmě nezablokuje, zabrání ale tomu, aby zlí současníci použili zadní vrátka k nalákání na jiné stránky nebo k instalaci obtěžujícího spywaru bez dotazu.

Když se chcete podívat na seznam zlých serverů, které zapsal IESPY-AD, podívejte se jednoduše do "Nastavení | Možnosti internetu | Bezpečnost | Omezené servery | Servery".

Neprat

P3P zabrání spamu

Výhonky reklamy a spamu zachází i podle zodpovědných osob příliš daleko. Nový přístup: sběratelé dat hrají s otevřenými kartami, prohlížeč kontroluje bezpečnost.

TAK FUNGUJE P3P - NOVÝ STANDARD PRO VAŠE SOUKROMÍ

P3P je zkratka pro "Platform for Privacy Preferences", tedy zhruba "platforma pro nastavení ochrany dat". Za tím se schovává technika postavená na standardu XML, s níž může každý provozovatel webového serveru určit vlastní směrnice ochrany dat.

Webové stránky, které jsou konformní s P3P, mají soubor XML s těmito nastaveními a sdělují uživateli, co s daty zamýšlejí. Ve směrnicích je například napsáno, jaký druh dat je sbírán, tedy informace pro kontakt online, jako je e-mailová adresa nebo hned kompletní poštovní adresa. Prohlížeč konformní s P3P porovná tento XML soubor s nastaveními uživatelů a učiní odpovídající opatření, tedy data sdělí, nebo ne. Opačně může webový server informovat uživatele, pokud požadavky na sdělení informací o uživateli nesouhlasí s nastavením prohlížeče a určité služby jsou případně zamítnuty.

Právě proto je standard P3P také sporný. Kritikové si stěžují, že formulace směrnic v XML je pro webmastery příliš složitá. Kromě toho prý musí každý uživatel dát na vědomí svá nastavení ochrany dat, než vůbec smí přistoupit na nějakou stránku a to i tehdy, když si chce jen přečíst pár informací. Pokud určitá stránka pak ještě ve svých směrnicích ochrany dat vyžaduje poštovní adresu, ačkoli si uživatel chce jen něco přečíst, zůstane přístup zablokován, dokud čtenář nesdělí svou adresu nebo nevypne funkci P3P. To nedává smysl ani pro provozovatele stránky, ani pro zákazníka.

Přitom by měl standard P3P vlastně fungovat téměř automaticky, neboť potřebné informace se ve většině případů stanovují přes cookies. Tak můžete v IE určit, které cookies chcete povolit, a které ne. Postup s P3P je ale naladěn jemněji a tím je vhodnější než obecné blokování cookies. V Internet Exploreru 6.0 najdete nastavení P3P v nabídce "Nastavení | Možnosti internetu | Ochrana dat". Zde můžete zhruba formulovat své přání k ochraně dat. Ve čtyřech stupních určíte, jestli všechny cookies přijmete, nebo - v opačném extrémním případě všechny cookies chcete zablokovat.

Podle informací odborníků na ochranu dat toto zdánlivé úplné blokování ale není účinné, neboť není nasměrováno proti anonymně nastaveným cookies. Provozovatelé reklamy tedy mohou přes existenci směrnic uložit cookies a tím informace o vašem chování při surfování.

P3P V PRAXI: OCHRANA DAT PRO PROHLÍŽEČ S JAP

Pokud kladete důraz na více bezpečnosti než nabízí Internet Explorer, měli byste si sepsat vlastní směrnice ochrany dat podle zvyklostí P3P a ty importovat do Internet Exploreru. Abyste si ušetřili práci při psaní a manipulaci s XML, sáhněte nejlépe po XML souboru připraveném bezpečnostním nástrojem JAP. Soubor stáhnete z adresy http://anon.inf.tu-dresden.de/ie6_privacy.html. Pro instalaci směrnic z tohoto souboru zvolte "Nastavení | Možnosti internetu | Ochrana dat", klikněte na "Import" a vyberte stažený konfigurační soubor.

U prohlížeče Opera je podpora P3P plánována bohužel až pro jednu z příštích verzí, Mozilla 1.5 naproti tomu již teď nabízí vypilovaný nástroj P3P. Zde jednoduše zvolíte "Editace | Nastavení | Ochrana dat & Bezpečnost | Cookies".

Vedle možnosti "Aktivovat cookies na základě bezpečnostních nastavení" kliknete na "Náhled" a pak můžete na vlas přesně nastavit, které cookies chcete kdy a především kde akceptovat.

Martin Goldmann, autor@chip.cz

MÉNĚ REKLAMY - VÍCE PROBLÉMŮ?

Při vší radosti z webových stránek očištěných od reklamy - tyto triky mají také své stinné stránky: prohlížeč si stěžuje kvůli údajným chybám, na webových stránkách je sotva možná navigace, aktualizace jsou ztíženy.

Některé funkce, které antireklamní triky vypínají, mohou být veskrze smysluplné. Dávejte proto při problémech se surfováním pozor především na následující omezení: Smysluplná pop-up okna jsou zablokována. Jako příklad lze uvést Amazon - kdo poprvé navštíví tento server, dostane vlastně pop-up okno s šekem na 5 eur. Také banky a servery se soubory ke stažení používají pop-up okna, aby získaly potvrzení pro přihlášení nebo pro spuštění downloadu. Bez pop-up oken tu nefunguje nic.

Používejte proto pro bankovní servery nebo právě pro Amazon konfigurovatelné blokování pop-up oken z nástrojové lišty Google, aby "pop-up okna serveru" byla v prohlížeči pro tyto adresy povolena. Žádný update bez ActiveX: Také vypnutý ActiveX může mít následky. Typickým příkladem je Windows Update. Pokud je ActiveX vypnutý, nemůže služba Update zjistit, které záplaty jsou na vašem počítači již nainstalovány.

Přidejte proto Update server pro Windows (http://v4.windowsupdate.microsoft.com/) k "důvěryhodným serverům" a aktivujte pro tuto zónu ActiveX.

Chybová hlášení bez ActiveX: Internet Explorer reaguje velmi podrážděně, když je ActiveX deaktivován. Na mnoha stránkách vyskakují chybová hlášení prohlížeče - dokonce i když příslušná stránka je vlastně zobrazena zcela korektně.

Žádná navigace bez Javy (JavaScriptu): Mnoho webových stránek používá Javu a JavaScript pro rozbalovací nabídky nebo rozložitelné podstránky - bez Javy pak nic nejde. Také internetové bankovnictví přes Java applet se takto znemožní.

Problémy s přihlášením bez cookies: Kdo zakáže cookies, ztratí výchozí nastavení pro přihlášení nebo se - i když jen velmi zřídka - na některé stránky vůbec nedostane. Přesto: Ukládání hesel na PC prostřednictvím cookie skrývá vysoké bezpečnostní riziko, a nemělo by se proto dít.

ZBAVTE SE REKLAMNÍCH E-MAILŮ

Stahování a třídění reklamních e-mailů je protivné a trvá dlouho. Co se tedy nabízí více, než svěřit tuto práci programu, který spam automaticky vytřídí? Majitelé Mozilly nebo její e-mailové odnože Firebird to mají skutečně jednoduché: chvíli trénují vestavěný spamový filtr a nevyžádané zprávy spolehlivě odstraní z došlé pošty. Pro všechny ostatní se nabízí POPFile (http://popfile.sourceforge.net). To je spamový filtr, který se zapojí mezi váš e-mailový program a vaši schránku POP3. Jakmile vyzvedáváte e-maily, přihlásí se váš e-mailový program u POPFile, který pak zprávy stáhne ze serveru.

Než tento nástroj předá poštu vašemu e-mailovému programu, prověří obsah. Podle kategorie následně POPFile označí zprávy. Na základě tohoto označení může e-mailový program jako Outlook Express zprávy třídit a přesunovat do složek.

POPFile na to ovšem potřebuje trochu tréninku. Pokud první spamové e-maily nezůstaly viset ve filtru POPFile, musíte je přiřadit ručně. Na základě tohoto přiřazení rozhodne POPFile, jak bude nakládat s dalšími zprávami tohoto obsahu. Čím častěji program trénujete, tím lépe později samozřejmě rozezná nevyžádané spamové e-maily.

POPFile je sice jedním z nejlepších spamových filtrů, nicméně programy jako tento nejdou po kořenu problému. Jakmile reklamní zprávy trčí ve vaší schránce, přece už způsobily škodu, neboť aby zaúčinkovala spamová funkce vašeho e-mailového programu, musí být zpráva přenesena na váš počítač.

Lepší je zastavit spamovou poštu již na e-mailovém serveru. Lepší poskytovatelé nabízejí takovou spamovou ochranu v dnešní době již sami.

ICQ BEZ REKLAMY

ICQ je plné reklamy. Při každém rozhovoru v internetu blikají nad tímto klientem reklamní obrázky. Abyste tomu zabránili, musíte ICQ trochu přestavět. Podrobný návod i potřebný soubor záplaty najdete na internetu na adrese http://www.michael-prokop.at/internet/icq.html.

PODLÉ TRIKY DIALERU ACTIVEX

Kdo používá Internet Explorer a má zapnutý ActiveX, je v nejvyšším nebezpečí, neboť pomocí tohoto rozšíření prohlížeče se mohou dialery dokonce samočinně a bez vašeho vědomí stáhnout a začít své drahé vytáčení.

Nejdříve se přitom přes ActiveX na vašem počítači uloží malý spouštěcí program. Pro ten se za určitých okolností dokonce ještě objeví okno varování a potvrzení. To pouze říká, že se má instalovat "komponenta". Označení jako "bezpečnostní update" nebo "update softwaru" mají skutečný účel jen zakrýt. Pro sebe vydané certifikáty předstírají bezpečnost a spolehlivost, avšak - každý, kdo zaplatí, dostane certifikát, nezávisle na účelu. Jakmile tedy s tímto downloadem souhlasíte, už je příliš pozdě, protože řídicí prvek ActiveX může z vašeho počítače libovolně stahovat další programy a nepotřebuje žádná dodatečná potvrzení.

Osud tak běží svou cestou. Jako další je stažen dialer, který se hned aktivuje. I když ho smažete, zůstane program k dodatečnému stažení, který při další příležitosti znovu obstará z webu dialer. Stahovací program navíc může výrobce dialeru zapsat do Internet Exploreru jako důvěryhodného, takže při dalších stahováních dialerů se již vůbec nebude na nic ptát.

Proti tomu pomůže jen jediné: vypnout ActiveX. Kromě toho kontrolovat v nabídce "Nastavení | Možnosti internetu | Obecné | Nastavení | Zobrazit objekty", které řídicí prvky ActiveX jsou aktivní. Nástroje jako YAW také pomohou proti dialerům. Tento a jiné programy najdete na adrese http://www.dialerschutz.de.

OD VÝROBCE BEZ REKLAMY - ALTERNATIVY K IE

Internet Explorer Microsoftu možná dominuje trhu, nejlepší prohlížeč proti spamu a reklamě to ale není. Zde má Mozilla jasné výhody, neboť do tohoto prohlížeče open source je již zabudováno blokování pop-up oken. Kromě toho můžete dokonce specifikovat načítání obrázků pro jednotlivé webové stránky.

Pro aktivaci blokování vyskakovacích oken v Mozille zvolte "Editace | Nastavení | Ochrana dat & Bezpečnost | Pop-up okna". Tady zapněte možnost "Blokovat nevyžádaná pop-up okna". Pod volbou "povolené servery" můžete navíc zapsat výjimky blokády.

Chcete-li navíc blokovat také bannery, klikněte v Mozille pravým tlačítkem myši na rušivou reklamu. Jedním kliknutím na volbu "blokovat obrázky z tohoto serveru" je server pro bannery odstaven. Musíte ovšem dávat pozor: pokud zobrazení přichází ze serveru, na němž si právě prohlížíte stránky, nebudou již vidět vůbec žádné obrázky. V tomto případě zvolte "Editace | Nastavení | Ochrana dat & Bezpečnost | Obrázky | Správa oprávnění obrázků". Tam příslušný server opět povolte.

Druhá alternativa k IE pochází ze Skandinávie: Opera. Tento prohlížeč blokuje pop-up okna dokonce ještě rychleji než Mozilla: stiskněte jednoduše klávesu F12 a zvolte podle chuti "odmítnout popup okna" nebo "otevírat jen vyžádaná pop-up okna". Tak máte také u Opery klid od obtěžujících trapičů. Abyste ovšem Operu učinili zcela reklamy prostou, měli byste zvolit placenou verzi programu, neboť jinak bliká vpravo nahoře v okně vždy reklamní banner - přes blokování pop-up oken.