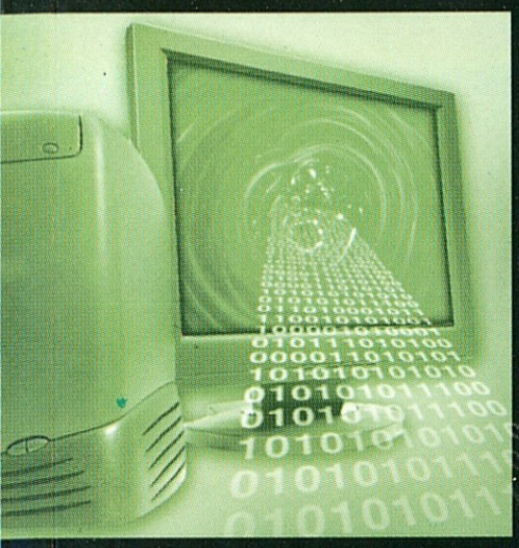


100%-OS PC VÉDELEM

TÉNYEK
TITKOK
TIPPEK

Computer
PANORÁMA

100%-OS PC-VÉDELEM

TÉNYEK,
TITKOK,
TIPPEK

Computer PANORÁMA

Figyelem! A könyvben látható kis CD-szimbólumok arra utalnak, hogy az adott bekezdésben szereplő programok a kiadványhoz tartozó CD-mellékletre is felkerültek.

Felelős kiadó: Dely Tamás ügyvezető igazgató
Szerkesztő: Horváth Annamária
Tervezőszerkesztő: Iszkra Ildikó
Címlapterv: Szincsák László

A kötetet készítette:
Levilágítás: HVG Press
Nyomtatta és kötötte: Kaposvári Nyomda Kft. – 231392
Felelős vezető: Pogány Zoltán igazgató
ISBN 963 7639 34 9

TARTALOM

1 Kéretlen levélszemét

Ha csak egy-két reklámlevelet kell kitörölnünk időnként a postafiókunkból, az még elviselhető. Mára azonban a levélszemét (idegen szóval: a spam) tömegjelenséggé vált, és mindenkit idegesít. Ebben a fejezetben közelebbről is bemutatjuk a spam-eket.

Önök is kaptak az utóbbi időben levelet *Jennytől*, aki be akarta mutatni Önöknek az új honlapját? A *Yahoo.de* domainről érkezett az üzenet, és a benne található link közvetlenül egy tárcsázó installációjához vezetett? Nos, biztosak lehetnek benne, hogy a feladó nem hús-vér ember, hanem egy robot volt.

1.1 A spam-mailek felismerése

Milyen egy spam-mail? Akad néhány kiindulási pont, amelyek alapján biztonsággal felismerjük a reklámszemetet.

Ellenőrizzük a *Címzett:* mezőt! Ha itt nem található meg a nevünk, az arra utal, hogy nem kívánatos mailről van szó. A törlésre kijelölés előtt azért ellenőrizzük még egyszer, hogy nem jött-e például a levél egy általunk megrendelt hírlevél küldőlistájáról. További ok a gyanakvásra a *Feladó* mező tartalma. Ha valaki teljesen ismeretlenül ír nekünk, az lehetne nagyon kedves is tőle, a legtöbb esetben azonban spam-mailről van szó.

A *Tárgy* mező is érdekes lehet. Ha ebben valaki ajándékozni akar valamit, ki a levéllel. Ha általában nem folytatunk külföldi levelezést, akkor minden olyan fejlécet jelöljünk meg törlésre, amely angol nyelven íródott. Az olyan *tárgyról* is lemondhatunk, mint „Szex", „Júlia 18" és hasonlók.

1.1.1 A spam-mailek leggyakoribb témái

A spam-mailek osztogatói többnyire gyorsan szeretnének pénzt keresni. Így azután ezeknek a maileknek a leggyakoribb témái a következő területekről származnak:

- Hitelközvetítés hitelképesség-vizsgálat nélkül, díjazás ellenében, amit természetesen előre kell fizetni,
- otthoni munka, amelyhez először termékeket kell vásárolnunk, hogy részt vehessük benne,
- gyógyszerek és erősítőszerek minden fajtájának kínálata,
- pornográf tartalmak felhívással egy képnézegető program letöltésére. Ezek mögött gyakran egy tárcsázó program rejtőzik emelt díjas telefonszámmal – ez sokba kerülhet!

A jövőben még biztosan jó néhány téma eszébe fog jutni a spamíróknak, amelyekkel átverhetnek bennünket. Semmi esetre se válaszoljunk az ilyen e-mailekre, mert abból a feladó tudni fogja, hogy a címünk használatban van.

1.2 Spam-botok telítik a hálózatot

Az ilyen spam-botok esetében olyan programokról van szó, amelyek önállóan hoznak létre postafiókokat freemail-szolgáltatóknál, és ezeket mint feladócímeket használják tömegesen elküldött mailjeikhez. A spamek küldői egyrészt így próbálják meg kicselezni a gyanútlan felhasználókat, akik megbízhatónak tartják az ismert szolgáltatótól érkező e-maileket. Másrészt a spam-botok gondoskodnak arról, hogy mindig újabb és újabb feladói címekről küldjék el a bosszantó reklámüzeneteket. Ezzel a módszerrel túljárnak azon felhasználók eszén is, akik levelezőprogramjuk tiltólistáival szűrik ki a spameket.

A spam-botok persze nemcsak az interneten szörfözőket bosszantják, hanem az adott szolgáltató hitelét is rontják. Ezért a szolgáltatók megpróbálnak különböző lépéseket tenni ellenük. A Yahoo!-nál például egy új e-mail account létrehozásakor lejátszódó regisztráció során egy olyan szót kell begépelni egy kis mezőbe, amely egy mintás alapon alig olvasható. A Yahoo! ezzel teszteli, hogy egy ember vagy egy gép jelentkezik-e be, a spam-botok ugyanis nem képesek azonosítani az elmosódott szavakat. Az eljárást a pennsylvaniai egyetemen dolgozták ki, és *Captcha* névre keresztelték.

A spam-botok, a hamis mail-accountok és a reklámtámadások egyértelműen tömegjelenséggé váltak. A **marketagent.com** piackutatóinak állí-

tása szerint az internetet használóknak mindössze 7 százaléka nem kap egyáltalán semmiféle reklámlevelet, míg a megkérdezettek negyede hetente több mint 20-at kap. A harmaduk maximum ötöt, s több mint egyharmadukat pedig akár heti 20 kéretlen e-maillel is bosszantják. A megkérdezettek 70 százaléka válaszolta azt, hogy ezeket az üzeneteket olvasás nélkül törli, míg több mint 20 százalékuk elolvassa, mielőtt kidobná a kukába.

A szörfözők 71 százaléka zavarónak tartja a spamet, csak 2,4 százalékuk vélekedett úgy, hogy egyáltalán nem érzik terhesnek a leveleket.

Érdekes kérdés az is, hogy milyen tartalmúak a spamek: a megkérdezettek 71 százaléka kap reklámszemetet az „Erotika és pornográfia" témakörből, több mint 51 százalékukhoz érkeznek ezen kívül flört- és társkereső ajánlatok is.

1.3 Dobozos hús és tömegmail

A spam neve, bármilyen meglepő is, egy húskonzervtől származik

A spam történetében az egyetlen vidám pont az elnevezés eredete: a név az amerikai *Hormel Foods* cég húskonzervének a nevéből származik: „**Sp**iced **Ham**". A „fűszeres sonkát" 1937 óta gyártják. Kezdettől fogva olcsó volt, tápláló és hosszan eltartható, ezért tömegesen fogyasztották. A

„Spam" húskonzerv a minden mást kiszorító tömegárucikk szinonímájává azonban csak a brit *Monty Python* komikus csoport egyik szösszenete révén vált, amelyben egy házaspár a büfében kizárólag spammel felszolgált ételeket kap, és egy viking-kórus a reklámból „spam-spam-spam" dalokkal kíséri a jelenetet.

Amikor felbukkantak az első végtelen számban sokszorosított mellékletek a hírcsoportokban, azokat a spamhez hasonlították. Később átterjedt a hasonlat a tömegmailekre is. A *Hormel* cég lazán fogja fel a dolgot, és **www.spam.com** webcímen működteti honlapját, amelyre egyre érkeznek a zaklatásnak kitett e-mail-felhasználók újabb és újabb dühkitörései.

A Homel céget nem érdeklik túlságosan a felháborodott e-mailek

1.4 A levélszemét kezdetei

A spam, azaz a levélszemét nem számít újdonságnak, jószerével egyidős az internettel. A levélszemetet udvariasabban „kéretlen kereskedelmi e-mailnek (Unsolicited Commercial Email – UCE)" vagy „kéretlen tömeg-e-mailnek (Unsolicited Bulk Email – UBE)" is nevezik. A nagy tömegben elküldött, előzetes kérelem vagy hozzájárulás nélküli e-mail angol neve a „spam". Az internet kezdetén a „spam" szót a kisebb-nagyobb cégek által saját termékeik és szolgáltatásaik reklámozása céljából elküldött levélözönre használták általánosan. A marketingcégek kezdetben rákaptak az

internetes levelek reklámlevél céljára való alkalmasságának, mint a sok ezernyi felhasználó olcsó elérési módszerének kihasználására. Gyorsan rájöttek azonban arra, hogy ez az új tömegkommunikációs forma zavaró, nem hatékony, elriasztja a vevőket, különösen, ha kéretlenül kapják.

A spam mellett alternatív módon használják a „junk" (szemét, hulladék) elnevezést is. A Microsoft például speciális szűrőlistákat hozott létre az Outlookban a junk e-mailekhez, és különbséget tesz a reklám és a „fiatalkorúakat veszélyeztető tartalmak" között. Amúgy a „junk" szó is a gasztronómia területéről ered: harminc évvel ezelőtt a *Time* magazin az egyik tudósításában arról panaszkodott, mennyire terjed az Egyesült Államokban az egészségtelen „junk food". Azt már nem tudjuk, hogy ki alakította ki később a „junk food"-ból a „junk mail" elnevezést.

A mai reklámszemétküldők sajnos nem törődnek a cégről alkotott képpel vagy a márka védelmével, egyszerűen csak a nagyon gazdaságos tömegmarketing-kampány néhány ezreléknyi válaszolási aránya érdekli őket. Ennek következménye az a nem kívánt e-mail-áradat, amely eldugítja a levélszervereket és ingerli a felhasználókat.

1.5 A levélszemét bűze

Az elmúlt másfél év alatt komoly problémává vált a levélszemét, amely például az Egyesült Államok teljes bejövő e-mail forgalmának 30-50 százalékát teszi ki, mi több, a legfrissebb adatok szerint ez inkább az 50 százalékot közelíti. Ennek következtében a vállalati hálózatok kereskedelmi érték nélküli levelek ezreit kénytelenek feldolgozni és tárolni, a vállalatok informatikai részlegei külön időt, energiát és pénzt kénytelenek a levélszemétnek a munkahelytől való távoltartását szolgáló megoldások keresésére fordítani.

De miért is facsarja a levélszemét szaga a vállalatok orrát? A válasz egyszerű:

- A levélszemét eldugítja a szervereket és az asztali gépeket, számítástechnikai erőforrásokat köt le.
- A levélszemét csökkenti a felhasználók termelékenységét, hiszen időbe telik a jó és a rossz e-mailek szétválogatása. A levélszemét emellett a rendszergazda és a segélyszolgálat idejét is rabolja.

- A levélszemét bosszantó, a visszataszító levelek pedig felháborodást okoznak.
- Számos spam-levél képe és szeméremsértő tartalma jogi következménnyel is fenyeget.

A Ferris Research becslése szerint a levélszemét ebben az évben várhatóan 10 milliárdnál is többe fog kerülni az Egyesült Államok-beli szervezeteknek. Ez a szám a kiesett termelésből és a levélszemét leküzdésére használt járulékos berendezések, szoftverek és persze az idő értékéből tevődik össze.

1.6 Tárcsázó és spam

A kéretlen e-mailekre napjainkban nem csak a tömeges terjesztés a jellemző. A spamek komoly veszélyt jelentenek azáltal, hogy egyre több pornográfiával és szexuális kapcsolatokkal foglalkozó oldalt reklámoznak. Ezeken a területeken rengeteg pénzt lehet keresni drága telefonszámokkal és olyan webtárcsázókkal, amelyek horribilis összegű kapcsolási díjakat számláznak. Mivel az internetezők többsége ismeri ezeket a veszélyeket, a feladók egyre rafináltabban járnak el és már-már tökéletesen álcázzák magukat.

Vannak olyan spam-küldők, akik olyan tömeges e-maileket küldözgetnek, amelyek ártalmas tárcsázókhoz vezető linkeket tartalmaznak. Feladóként „Jenny", „Claudia" vagy „Sindy" címei szerepelnek, akik állítólag első honlapjukat készítették el és e honlapok bemutatójára invitálnak bennünket. Ezek a spam-mailek is megtévesztően valódinak tűnnek. Ha például valakinek van Claudia nevű ismerőse (és hát nem kevesen vannak ilyenek), hamar besétál a csapdába egy ilyen szöveget olvasván: „Tudni akartad, hogyan érhetsz el. Itt olvashatod a weboldalam címét: … Szia, írj minél előbb! Claudia".

Az ilyen üzenetek nem csupán megtévesztően valódinak látszanak, hanem kimaradnak belőlük a spamekre jellemző „kulcsszavak" is, mint például „szex", „ingyen" vagy „milliomos". Ezért az antispam szoftverek vagy az Outlook szokásos szűrői nem ismerik fel, és a levelek a címzett számítógépére kerülnek.

1.7 Hogyan találnak ránk a spam-küldők?

A levélszemetelők általában az alábbi módszereket használják az e-mail címlista létrehozására:

- **Az internet.** Az összes e-mail-cím, amelyet elküldenek vagy fellelhető az interneten, célpontnak számít. A levélszemetelők az internet számtalan forrásából gyűjtik össze az e-mail-címeket: a webhelyekről, a böngészőkből, a szaknévsorokból, az internetes telefonkönyvekből, de az IRC-ből és a csevegőszobákból is. A hírcsoportokba küldött közlemények is a levélszemetelők forrásául szolgálnak.
- **A listák kereskedelme.** A „listaügynökök" e-mail-listákat adnak el jó pénzért a levélszemetelőknek. A levélszemetelők egymás közötti listakereskedelme is mindennapos. Nyugodtan elmondhatjuk, hogy ha egyszer egy e-mail-cím felkerül egy listára, hamarosan megjelenik a többi levélszemetelő listán is.
- **Találgatás.** A címek kitalálása, más néven a „szótár módszer" is igen hatékony módja az e-mail-címek begyűjtésének. Ha például a gyakori keresztnevek elé vagy mögé biggyesztünk egy, esetleg több betűt, és olyan közismert levéltartományt használunk, mint például a *Yahoo.com*, vagy éppen a Fortune 5000 cégeinek tartományait, a levélszemetelő könnyedén létrehozhat sok ezernyi valódi e-mail-címet. A nem működő címekre fordított költség gyakorlatilag nulla. Vannak erre a célra kifejlesztett szoftverek is, amelyekkel ezt a módszert használva a levélszemetelők milliószámra hozhatják létre az e-mail-címeket.

1.8 A spam közvetítő közege

Az internetszolgáltatók legtöbbje szabályzatában megtiltja a felhasználóknak a levélszemét küldését, így a levélszemetelőknek gyakran titokban kell dolgozniuk, és más, általában lopott hálózati erőforrásokat kényszerülnek használni. A levélszemét főbb továbbítói:

- **A nyitott továbbítók.** A levélszemetelők felismerik az interneten a nyitott továbbítókat, és ezeket a szervereket használják tömegleveleik elküldésére, amellyel egyrészt elleplezik a levelek eredetét, és mint

„ingyenes" erőforrást használják a tömeglevelek kiküldéséhez. Ezeknek a levéltovábbítóknak a tulajdonosai többnyire tisztességes cégek, akiknél rosszul van beállítva a levélszerver.

- **A gazember (csirkefogó) internetszolgáltatók.** Egy „levélszemétház" a levélszemét továbbításából él. Ezek közvetlenül az internet gerinchálózatra csatlakoznak, a nagy adatátviteli szolgáltatóknak éppúgy fizetnek a szolgáltatásért, mint a tisztességes internetszolgáltatók. Ezek a levélszemetelők folyamatosan változtatják a tartománynevüket és az IP-alhálózatukat, hogy kivédjék a levélszemétszűrőket és a tiltólistákat, és szabadon küldik a levélszemetet szerte a világba.
- **Az egyszeri hozzáférések.** A levélszemetelők gyakran iratkoznak fel ingyenes vagy próba e-mail-hozzáférésre valamely nagy internet- vagy weblevél-szolgáltatónál. Mindaddig küldik a leveleiket erről a címről, amíg ki nem zárják őket, majd továbblépnek a következő ingyenes hozzáférésre.
- **Nyitott webproxy-k.** A rosszul beállított, „nyitott" proxy-k lehetővé tehetik a külső felhasználóknak, hogy hozzákapcsolódjanak a webszerverhez (például a 80-as porton) és egy véletlenszerűen kiválasztott levélszerverhez névtelenként hozzákapcsolódva levélszemetet tudjanak küldeni.
- **A vezeték nélküli internetkapcsolatok.** A vezeték nélküli kapcsolatok egyre inkább elterjedtté válnak, ezzel széles út nyílik a levélszemetelők számára a hálózati erőforrásokhoz való hozzáférésre.

2 Harc a spam-ek ellen

Az előző fejezetben megismerkedhettünk közelebbről is a spam-ekkel. Most viszont a kicselezésükhöz adunk ötleteket.

Ha csak egyszer is felbukkan valaki e-mail címe a spam-küldők listáin, akkor attól fogva ki van szolgáltatva a támadásoknak. Ilyenkor már csak a szűrők és az antispam toolok alkalmazásával tartható tisztán a postafiók.

2.1 Mit lehet tenni?

Bánjunk óvatosan e-mail címünkkel! Hozzunk létre egy vagy két további e-mail pstafiókot, és használjunk a címünkben álneveket vagy fantázianeveket! Névtelen accountokat használjuk, ha hírcsoportokban vitázunk, levelezőlistákra iratkozunk fel vagy olyan kapcsolatokat alakítunk ki, amelyekkel szemben még nem teljes a bizalmunk. A fő címünket használjuk viszont, ha a barátainkkal, ismerőseinkkel és üzletfeleinkkel kommunikálunk. Ezzel a fontosabb postafiókunkat tisztán tudjuk tartani, míg a névtelen accountot elárasztathatják a reklámok. Ha már túl sok van belőlük, akkor egyszerűen újabb álnevet választunk.

Ajánlatos elkerülni az e-mail címlistákat, például az Internetes Sárga oldalakat, ahol mint egy telefonkönyvben lehet e-mail-címekre keresni. Bármilyen praktikusak is ezek, ne feledjük: az ilyen mail-listák a spamek feladóinak elsőrendű forrásai a hírcsoportok mellett, amelyeknél minden résztvevő e-mail-címe könnyedén megszerezhető. Ezek a címek különösen értékesek, hiszen aki itt regisztráltatja magát, biztosan elérhető akar lenni, és rendszeresen megtekinti az e-mailjeit.

Amint felbukkannak a postafiókunkban az első reklámlevelek, csak a komoly cégek esetében éljünk azzal a lehetőséggel, hogy a mellékelt linkkel lemondjuk a kéretlen reklámüzenetek küldését. A spamek esetében soha ne használjuk az ajánlott linket, mivel ezáltal a spam küldője számára kiderül, hogy az e-mail-cím valódi és az üzenetet elolvasták. Ugyanezen okok miatt a panaszainkkal se forduljunk válaszlevélben a feladóhoz az e-mail programunk *Válasz* vagy *Reply* parancsával.

2.1.1 Antispam toolok

Ha mindezen biztonsági előírások sem elégségesek, és az e-mail accountunkat spam-mailekkel bombázzák, akkor állítsunk be szűrőszabályokat a mail-kliensünkhöz. Az Outlook és az Outlook Express alapján a következő oldalakon bemutatjuk, hogyan blokkolhatunk egyes feladói címeket illetve hogyan küldhetünk egyből a kukába bizonyos spammaileket. A szűrőszabályokat persze rendszeresen gondozni kell, mivel csak jellemző spam-szavakkal és -kifejezésekkel működnek, amelyek állandóan változnak. A „webcam" szót tartalmazó leveleket azonnal ki-

szűrhetjük, ám a korábban említett „Jenny"- vagy „Claudia"-féle üzenetek szűrőkkel is alig válogathatók ki.

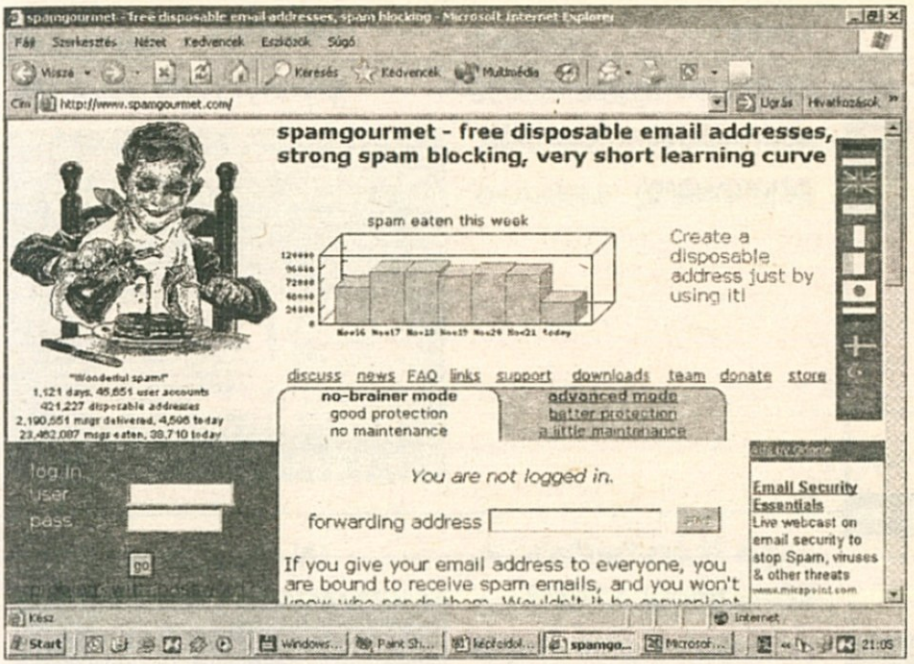
Itt mutatkoznak meg az antispam-programok erősségei. Feltéve, hogy rendelkezünk POP3 mail-postafiókkal, amellyel levesszük e-mailjeinket a szerverről, és elmentjük a számítógépünkre, ezek a toolok a szolgáltató és a mail-kliens közé kapcsolódnak a számítógépünkön. A programablakban először csak a beérkezett e-mail fejlécének az adatai jelennek meg (feladó, tárgy, dátum, méret stb.). Eldönthetjük, melyik mailt töltjük le a számítógépünkre, illetve töröljük a szerveren vagy vesszük fel a blokkolt mailek listájára. Ezzel a módszerrel kapcsolási költségeket takaríthatunk meg, és nem is engedjük a számítógépünkre a veszélyes linkeket vagy mellékleteket.

Sok ilyen, freeware-ként vagy shareware-ként terjesztett segédeszköz megtalálható az interneten, az ismert keresők segítségével. A kereskedelmi forgalomban lévő termékeknek néhány kiegészítő programfunkciójuk is van, mint például a „panasz-mail". A normális viszontválasszal ellentétben, a szerver hibajelentésével vezetjük félre a spam küldőit, akik azt a fiktív üzenetet kapják, hogy az e-mail-címünk nem létezik és így, ha szerencsénk van, lekerülhetünk a spam-listáról. Egyes programok esetében panasz-maileket juttathatunk el a szolgáltatóhoz is, és értesítjük, hogy a spam-küldők visszaéléseket követnek el.

Ezzel persze nem szűnik meg minden probléma. A spam-mailek ugyanis csak akkor tűnnek el a hálózatról, ha a költségeik már nem állnak arányban a várható nyereséggel. Mivel azonban a spam-akciók gyakorlatilag nem járnak költségekkel, nem számíthatunk gyors sikerre. Addig csak egyet tehetünk: ne menjünk bele a spam-tartalmakba.

2.1.2 Eldobható mailek és szűrőszolgáltatások

A reklámözön elleni harcban a saját számítógép tooljain kívül online szolgáltatások is segítenek. A **www.spamgourmet.com** weboldalon például „eldobható" címeket lehet összegyűjteni, amelyeket egyszeri használatra szánnak. Egyszerű séma alapján találjunk ki egy anoním címet, annak a szituációnak megfelelően, amelyben szükségünk van a működő e-mail accountra. A címet a SpamGourmet automatikusan beüzemeli az első beérkező üzenettel. Szükség esetén akár 20 e-mailt is továbbíttatha-



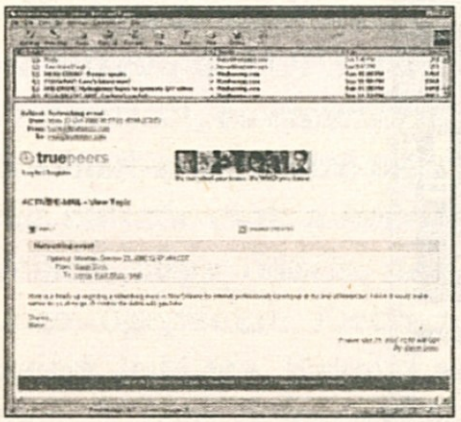
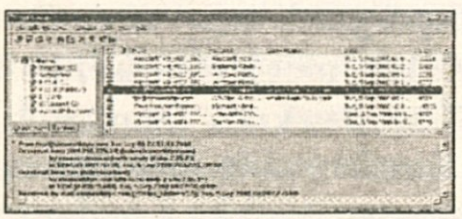
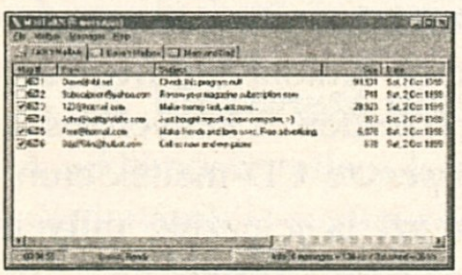
Itt lehet összegyűjteni „eldobható" e-mail-címeket

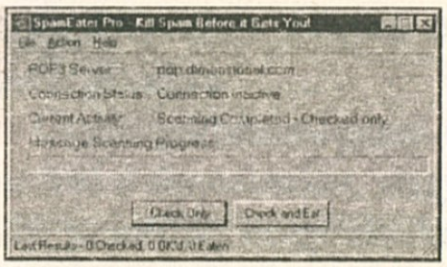
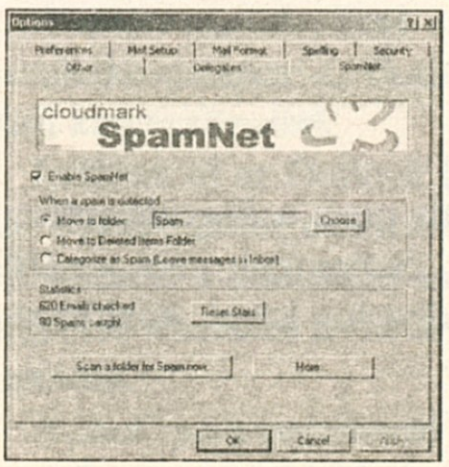
tunk a SpamGourmet-címről a báziscímünkre. A rendszer minden további (spam-) üzenetet „elnyel".

A **www.eleven.de** „eXpurgate" szolgáltatása privát felhasználóknak ugyancsak ingyenes. Egy e-mail-címmel be kell jelentkezni, amelyről minden beérkező üzenetet továbbítanak az „eXpurgate" szerverre. Ott nagyteljesítményű szűrők ellenőrzik az e-mailjeinket, megjegyzéssel látják el a fejlécben, majd tovább küldik a „tiszta" üzeneteknek fenntartott e-mail-címünkre vagy egy saját spam-címre.

2.1.3 Valóban hasznos antispam toolok

Az alábbi listán olyan antispam toolokat mutatunk be, amelyek megóvják a postafiókunkat a kéretlen reklámok áradatától. Különböző freeware és shareware programokról van szó, amelyek egyszerűen és kényelmesen letölthetőek számítógépünkre az internetről, de persze CD-mellékletünkön is megtalálhatók. A programnevek mellett azt is jelezzük, milyen nyelven (A=angol, N=német) áll rendelkezésre az adott szoftver.

Program	Leírás	Honlap
Active E-Mail Monitor 2.F (A) 	Kombinált e-mail monitor, spamvédelmi funkciók (shareware)	www.emailmon.com
E-Mail-Remover 3.0 (A) 	Közvetlenül a POP3 postafiókról törli a reklámokat és más zaklatásokat (freeware)	www.eremover.bizhosting.com
Mail Snoop 1.430 (A) 	Automatikus megválaszolja a spameket, ellenőrzi és szűri a beérkezett üzeneteket (freeware)	www.rainbow-innov.co.uk
MailTalkX 3.41 (A) 	Spam-szűrő és e-mail toolok	www.softbylabs.com

Program	Leírás	Honlap
PacSpam Pro 6.2.1 (N) 	Jellista alapján vizsgálja meg a levelezőszerveren lévő e-maileket (shareware)	www.heitho.de
Spam Buster 1.95 (A) 	A szűrőtechnikák egy speciális mappába továbbítják a reklám-üzeneteket (shareware)	www.contactplus.com
SpamEater Pro 3.65 (A) 	Címlista alapján ellenőrzi a levelezőszerveren lévő e-maileket (shareware)	www.hms.com
SpamNet 1.07e (A) 	Outlook-tool, Peer-to-Peer-hálózaton keresztül hozza létre a spam-küldők listáját (freeware)	www.cloudmark.com

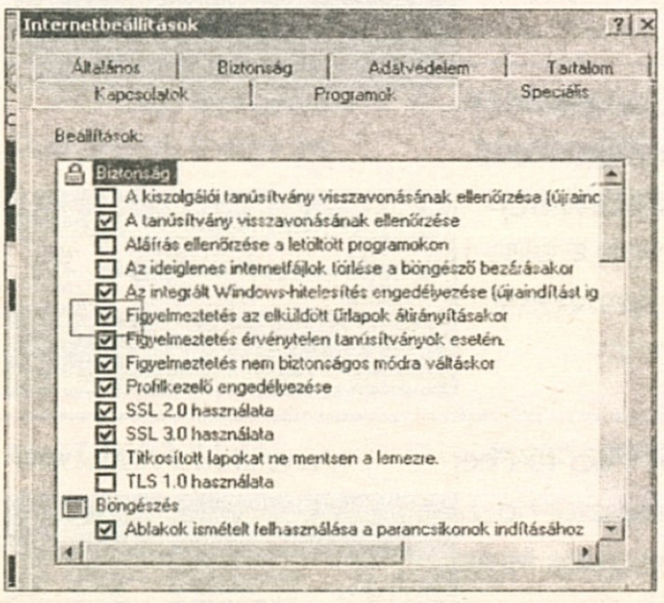
2.2 Ne adjunk esélyt a spam-nek!

Teljes egészében nem tudjuk száműzni a reklámokat a postafiókunkból. Tippjeinkkel és trükkjeinkkel azonban gátat szabhatunk a kéretlen üzenetek áradatának – csak néhány reklámlevél marad a postafiókban.

2.2.1 Ne küldjünk el űrlapadatokat!

Egyes weboldalak olyan scriptekkel dolgoznak, amelyek lekérdezik az internetes kapcsolat bizonyos adatait, amint arra az oldalra lépünk. Az oldalak üzemeltetői az úgynevezett űrlapadatokra kíváncsiak, amelyek közül különösen az e-mail-cím a fontos számukra. Ez a folyamat az internetes kapcsolat beállításainál letiltható.

Indítsuk el az Internet Explorert, és az *Eszközök* menüpontban nyissuk meg az *Internetbeállítások*-at. Aktiváljuk a *Speciális* regiszterlapot, és lapozzunk lefelé.



Figyelmeztetésre kérhetjük az Internet Explorert

Egérgombnyomással kattintva tegyünk egy kis pipát a *Figyelmeztetés az elküldött űrlapok átirányításakor* opció elé, és hagyjuk jóvá az *OK* gombbal. A későbbiekben a böngészőnk engedélyt fog kérni, mielőtt elküldené az internetkapcsolat adatait.

2.2.2 A feladó blokkolása

Ha mindig ugyanattól a feladótól kapunk spam-mailt, az Outlook Expressben blokkolhatjuk a feladó címét. Az érintett mailek ezután megkérdezés nélkül a *Törölt elemek* mappába kerülnek.

A bal egérgombra kattintva jelöljünk ki egy új spam-mailt a levelező programunk postafiókjában. Az *Üzenet* menüben válasszuk ki a *Feladó letiltása* parancsot.

Az Outlook Express ezzel az adott e-mail-címet felveszi egy „feketelistára". A következő párbeszédablakban megkérdezi a program, hogy azonnal törölje–e a kijelölt mailt. Az *OK* gombbal hagyjuk jóvá.

2.2.3 Az e-mail domain blokkolása

Az Outlook Express-szel nemcsak egyes mailek, hanem egész domainek is blokkolhatók, amelyekről rendszeresen kapunk spam-maileket. Ha például biztosak vagyunk abban, hogy a *@lycos.it* címről kizárólag spamet kaphatunk, akkor küldessünk minden *@lycos.it* e-mailt automatikusan a kukába.

Indítsuk el az Outlook Expresst és válasszuk ki az *Eszközök/Üzenetszabályok/Letiltott feladók listája* menüpontot, majd klikkeljünk a *Hozzáadás* gombra.

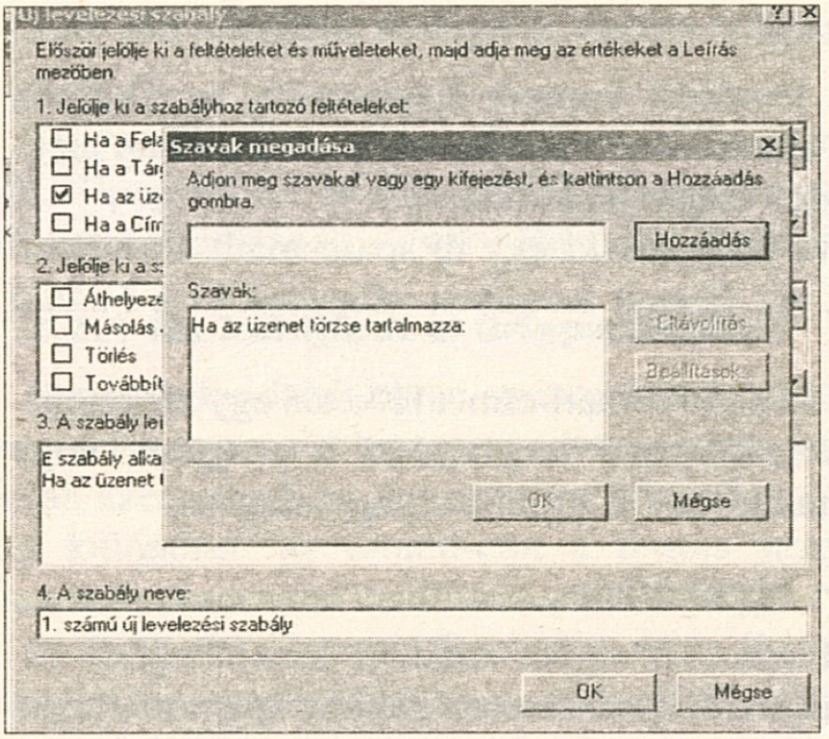
Újabb párbeszédmező nyílik meg, amelybe be kell írnunk a „@"-jel nélkül a domaineket, vagyis például: „lycos.it". Kétszer hagyjuk jóvá az *OK* gombbal, hogy blokkoljuk a domaint.

2.2.4 Spam-elleni szűrőszabályok alkalmazása

A spam-mailek elleni szabályok pontos definiálásához minták állnak a rendelkezésünkre az Outlook Expressben. Ezeket csak néhány változóval kell kiegészítenünk.

Indítsuk el az Outlook Expresst, és válasszuk ki az *Eszközök* menüben az *Üzenetszabályok/Levelezés* opciót. Ahhoz, hogy például a „hot" szót tartalmazó e-mailekkel szemben megvédhessük magunkat, kattintsunk a legfelső mezőben a *Ha az üzenet törzse a megadott szavakat tartalmazza* opcióra.

A „hot" szót tartalmazó spam-mailekhez válasszuk ki az alatta található mezőben a megfelelő akciót. Kattintsunk például a *Továbbítás a ... map-*



Ebben a mezőben adhatjuk meg a blokkolni kívánt szavakat

pába parancsra. Mindkét kiválasztott opció a legalsó párbeszédmezőben jelenik meg. A *Szöveg* és a „'…'" változók kék színnel kiemelten tűnnek fel.

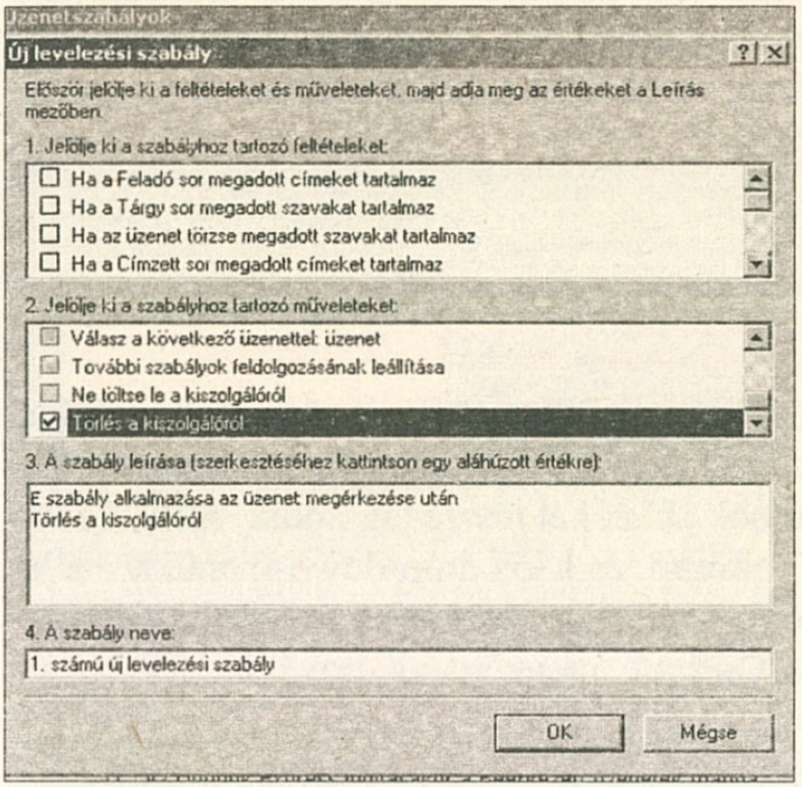
Kattintsunk a kék *Szöveg* bejegyzésre. Ekkor megnyílik egy újabb beírási mező, ahol a „hot" szót kell megadnunk. Hagyjuk jóvá a *Hozzáadás* gombra kattintva, és adjunk meg adott esetben akár további szavakat is, mint például „money". A párbeszédablak legalsó mezője felsorol minden bejegyzést. Nyugtázzuk ezeket az *OK* gombbal. Most már a *Szabályleírások* mezőben is megtalálhatók a fogalmak.

Ugyanígy járjunk el a kék bejegyzéssel a kívánt akció beállításához. A *Továbbítás* párbeszédablakban válasszuk ki a *Törölt elemek* mappát. Végül a *4. A szabály neve* sor alatt írjuk be a szabály választott nevét.

2.2.5 Spam törlése a letöltés előtt

Különösen hatékonyak azok a szabályok, amelyek közvetlenül a szerveren törlik a spam-maileket, mielőtt letöltenénk azokat a számítógépünkre. Ezáltal eleve nem tesszük ki magunkat annak a veszélynek, hogy a spam-mailekkel kártékony fájlokat vagy tárcsázó-letöltésekhez vezető linkeket mentünk a merevlemezre.

Járjunk el a szűrőszabályok beállításához hasonló módon, és válasszuk ki az *Eszközök/Üzenetszabályok* menüben a *Levelezés* opciót. Határozzunk meg egy új szabályt, vagy keressük meg a fennálló szabályok listáját a *Mégsem* gombbal. Jelöljük ki itt a kívánt szabályt, és kattintsunk az *Alkalmaz* gombra.

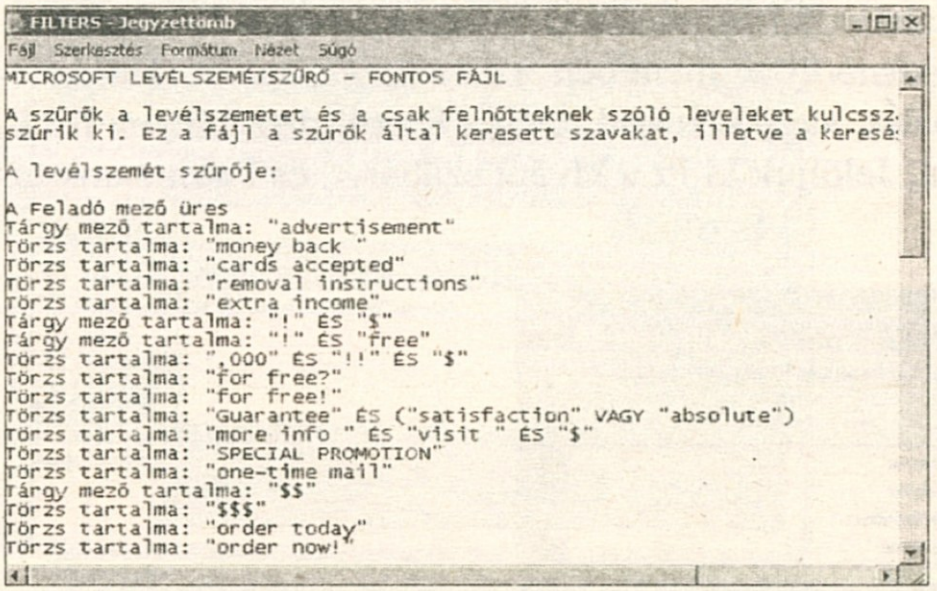


Akár rögtön a szerverről is töröltethetünk e-maileket

Lapozzunk lefelé a középső mezőben található opciókig. Tegyünk egy kis pipát a *Törlés a kiszolgálóról* akció elé. A legalsó mezőben adjunk nevet a szabálynak, és hagyjuk jóvá az *OK* gombbal.

2.2.6 A junk-mailek szűrése az Outlookkal

Az Outlook „junk-mail-rendező opciókat" is kínál. Itt olyan előre definiált szabályokról van szó, amelyekkel a spamek kiválogathatók. Ezek a szabályok a jellegzetes fogalmakat tartalmazó szólistán alapulnak. A *Microsoft Office/Office* mappában, a *Filters.txt* fájlban vannak elmentve a *Csak felnőtteknek (Adults only)* vagy a *Rendelje meg most (Order today)* szövegek. Mivel ez a lista kizárólag amerikai fogalmakat és címeket tartalmaz, a junk-mail-jegyzéket folyamatosan bővítenünk kell.



A Filters.txt fájl tartalma

Ahhoz, hogy a Microsoft előre definiált szabályait aktiváljuk, jelöljük ki a *Beérkezett üzenetek* mappát, és a *Speciális* menüben válasszuk ki a *Rendezés* opciót. Erre az Outlook ablak két részre tagolódik. A felső részben kattintsunk a *Junk-mail* feliratra, és a kis drop-down-menükkel állítsuk be, hogy a junk-mailt megjelöljük vagy át akarjuk helyezni. A *Bekapcsolás* gombra kattintva az Outlook megkérdezi, hová mentse az új, *Junk-mail* elnevezésű mappát.

Ha spam-mailt kapunk, jelöljük ki, és az *Akciók* menüben kattintsunk a *Junk-mail/Hozzáadás a junk-mail feladók-listához* vagy a *Hozzáadás az ifjúságra nem veszélyes tartalmak küldőinek listájához* bejegyzésre.

2.2.7 Speciális szűrés az ExLife-fal

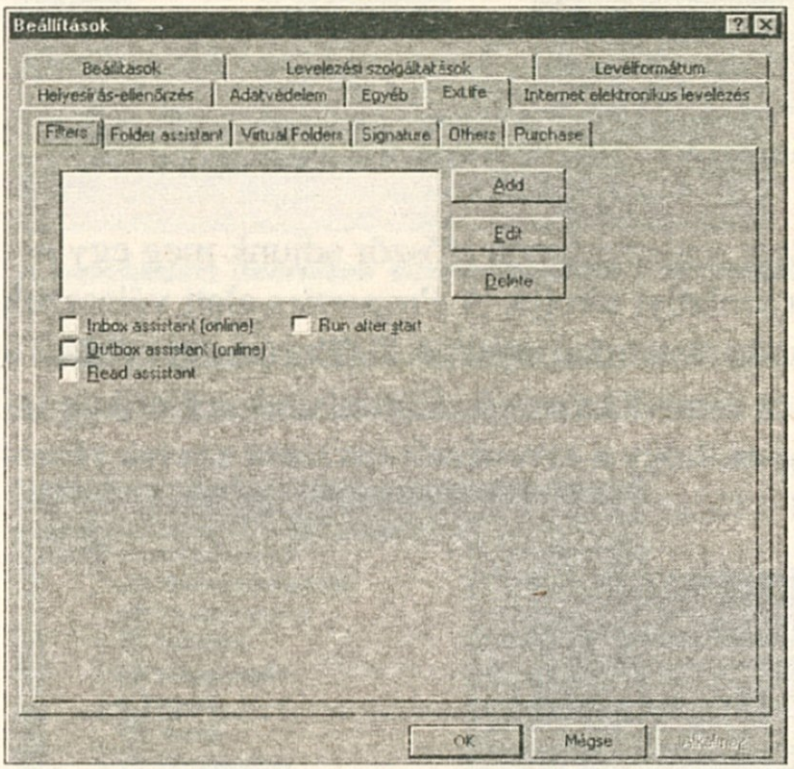
Ha nem elégségesek számunkra az Outlook szabályai, akkor azok az *ExLife* plug-in-nel bővíthetők. Ez a tool virtuális mappákat is készít, amelyekkel áttekinthetővé válik az elektronikus levelezésünk. Ha például sok olyan szabállyal dolgozunk, amelyek az új üzeneteket különböző mappákba továbbítják, akkor minden olvasatlan mailt megjeleníthetünk egy virtuális mappában.

Töltsük le a **www.ornicusa.com/old** weboldalról, illetve CD-mellékletünkről az ExLife aktuális verzióját. Az angolnyelvű tesztváltozat 30 napig teljes körűen működőképes, a licenc egy számítógéphez 30 dollárba kerül. A plug-in kompatíbilis az Outlook 97/98/2000-rel és a Windows

95/98/NT-vel. Mentsük el az önmagát kicsomagoló fájlt dupla kattintással a programmappánk saját könyvtárába. Az ExLife erre önállóan installálja magát az Outlookban.

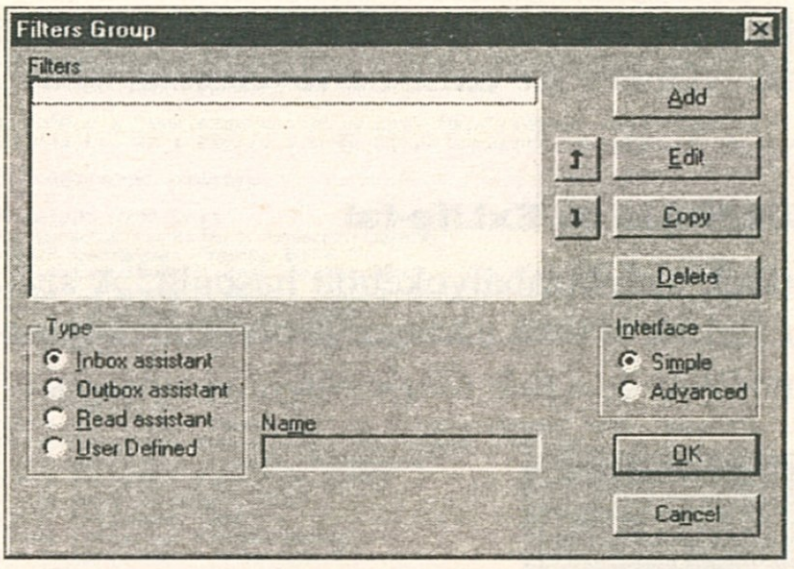
2.2.8 Szűrőszabályok előállítása az ExLife-fal

Az ExLife alapelve az Outlook szűrőszabályokéhoz hasonlít. A szabályvarázslóhoz hasonlóan az ExLife is több párbeszédablakkal támogat minket az új szabályok kialakításában és a már meglévők módosításában.



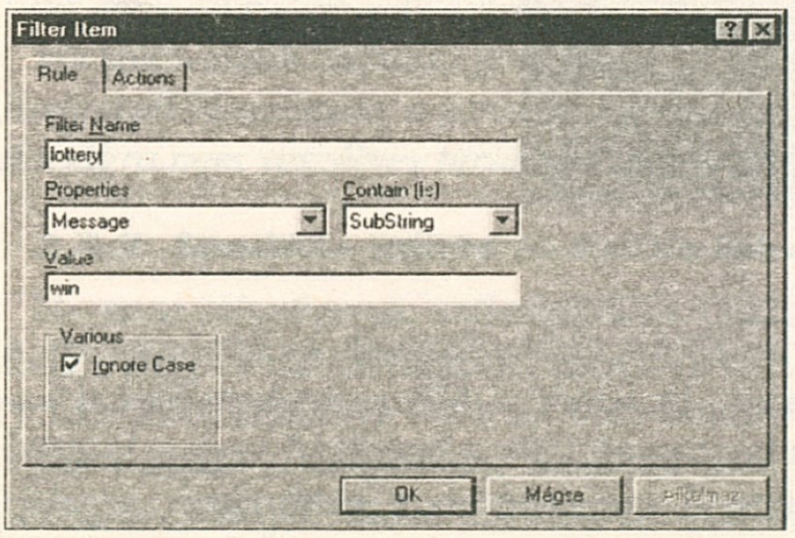
Itt hozhatunk létre új szűrőcsoportot

Válasszuk az Outlookban az *Eszközök/Beállítások* menüpontot, és a hozzáadott *ExLife* regiszterlapot. Itt ismét a *Filters* regiszterlapon vagyunk, ahol szűrőcsoportokat hozhatunk létre a beérkező vagy a kimenő postához. Az új szűrővel történő kiegészítéshez kattintsunk az *Add* gombra. A következő ablakban ügyeljünk arra, hogy az *Inbox assistant* be legyen kapcsolva, és kattintsunk még egyszer az *Add* gombra.



Az Inbox varázsló segít az új szűrőcsoport létrehozásában

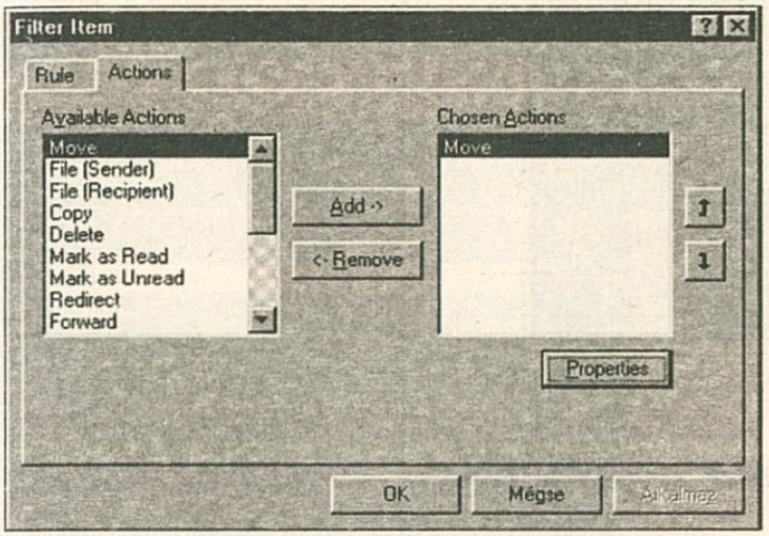
A következő ablakban, a *Rule* regiszterlapon először adjunk meg egy nevet, amely alatt az Outlook a szabályt tárolja. A *Properties* alatt válasszuk ki azt a helyet, ahol a fogalmat kerestetni akarjuk. A *To(Recipient)* például a címzettet jelenti, a *Message* az e-mail szövegét. Kattintsunk a *Contain* legördülő menüben a *SubString*-re, hogy a keresőszót összetett szavak részeként is azonosíttassuk. Végül a *Value* alatt írjuk be a keresőfogalmat.



A keresőszó megadása

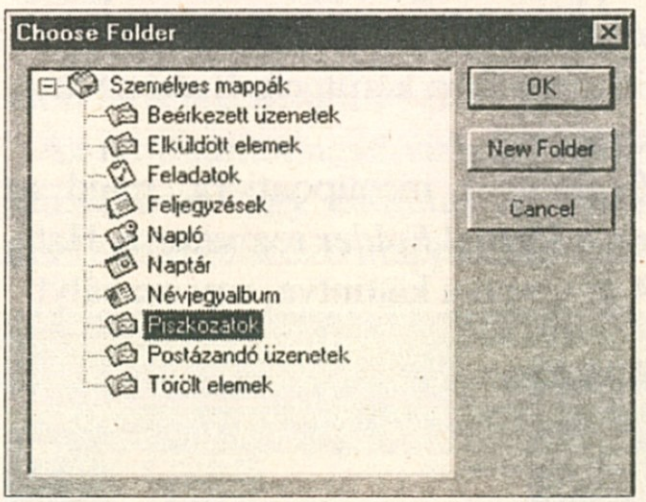
Hogy rögzítsük, mit kell tennie a szabálynak, menjünk az *Actions* regiszterlapra. Itt jelöljük ki a *Move*-ot, hogy az érintett e-mailek átkerüljenek egy másik mappába, vagy a *Delete*-et a törlésükhöz. Kattintsunk is-

mét az *Add* gombra, hogy a választásunk a bal oldali mezőből átkerüljön jobbra, a *Chosen Actions* mezőbe.



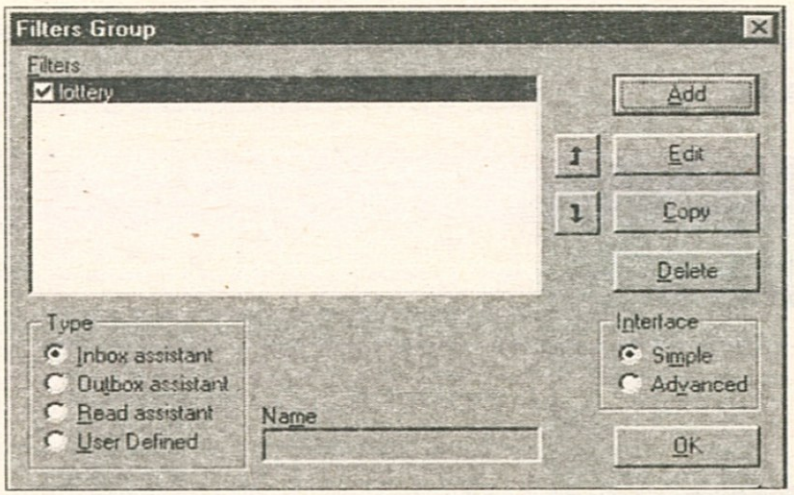
A beérkezett üzenetek automatikusan a kiszemelt mappába kerülnek

Ha a *Move* mellett döntöttünk, a *Properties* gombra kell kattintani, hogy kiválasszuk a célmappát az Outlook mappalistájából.



A célmappa kiválasztása

Miután minden szűrőszabályt beírtunk és jóváhagytunk, az ExLife készít egy bejegyzést a *Filters Group* ablakban. Hagyjuk jóvá ezt is OK-val. A plug-in erre beszúrja az *Inbox Assistant* csoportot a *Filters* regiszterlapra.

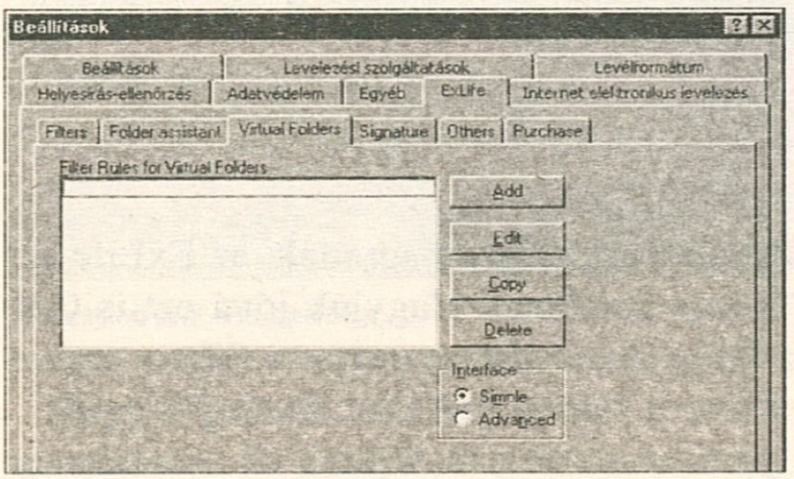


Munkára kész az új szűrőcsoport

2.2.9 Olvasatlan üzenetek ellenőrzése

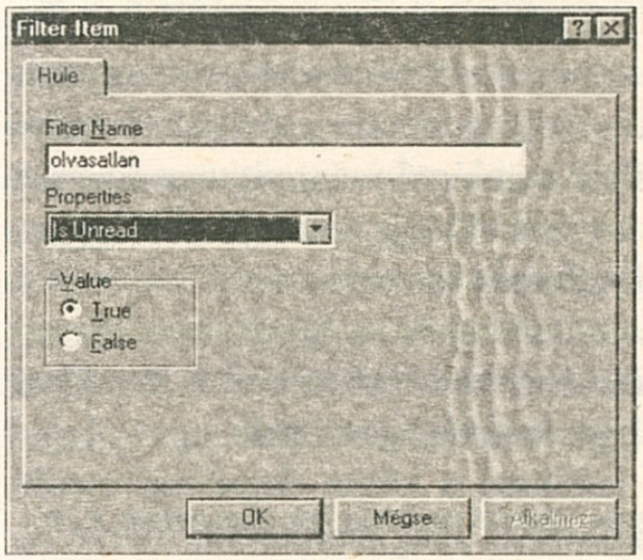
Hogy minden olvasatlan e-mailt egy helyen áttekintve tudjunk ellenőrizni vagy olvasni, az ExLife virtuális mappákkal dolgozik. Ha az e-mailjeinket az Outlookkal és az ExLife-fal szűrjük, és automatikusan almappákba helyeztetünk át üzeneteket, sok spamként megjelölt és ezáltal olvasatlan mail a *Törölt elemek* mappában fog landolni. De meghatározott feladók szűrőszabályok által továbbirányított üzenetei is elsőre olvasatlanok maradnak, hiszen speciális mappákba kerülnek. Ezért szükséges egy virtuális mappa a gyors áttekintéshez.

Menjünk az Outlook *Eszközök/Beállítások* menüpontjára, majd az *ExLife* regiszterlapra, és ott kattintsunk a *Virtual Folder* regiszterre. Határozzunk meg a szokásos módon, az *Add* gombra kattintva, egy szabályt.



Új szabály hozzáadása

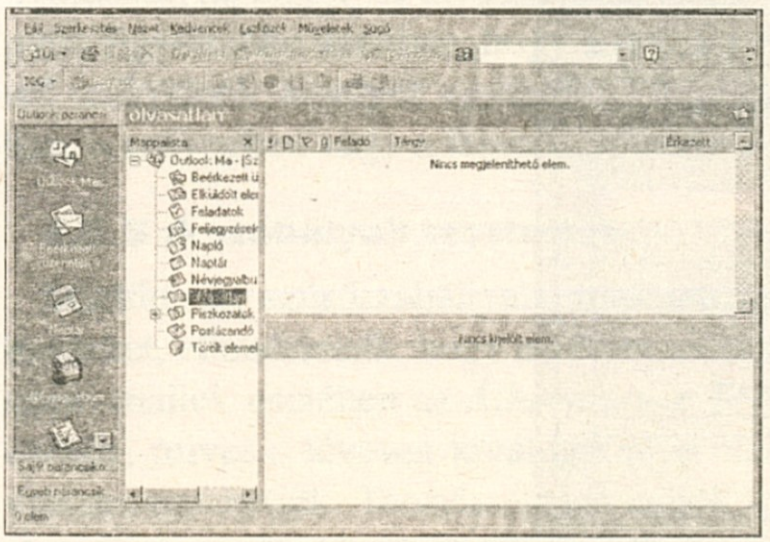
A *Filter Name* alatt írjunk be a mentéshez egy nevet, például *Olvasatlan*, és válasszuk hozzá a *Properties* legördülő menüből az *Is Unread* bejegyzést. Ezzel meghatároztuk az olvasatlan mail-eket. A többi beviteli mező eltűnik, csak a *True* opció erősíti meg az *Olvasatlan* szűrőfeltételt.



Nevet adunk a szabálynak

Kattintsunk az OK gombra. A program most beírja az új szabályt a megadott néven a *Virtual Folders* listába. Ezt az ablakot is OK-val hagyjuk el.

Az *Olvasatlan* nevű virtuális mappa most megjelenik az Outlook mappalistájában. Egy kattintás az Olvasatlanra, és megjelennek a mail-ek, amelyek különböző mappákban elszórva vannak tárolva az Outlookban.



A virtuális mappa az Outlook mappalistájában is megjelenik

2.3 További tippek és trükkök a spamek ellen

2.3.1 Az automatikus betekintő deaktiválása

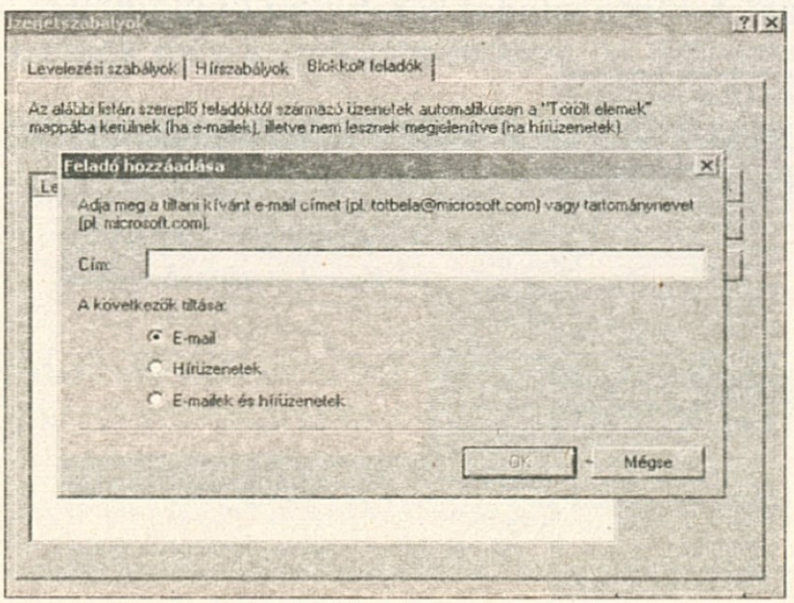
Ha kikapcsoljuk e-mail programunkban *az automatikus e-mail betekintőt,* bebiztosíthatjuk magunkat a kártékony scriptekkel és rejtett vírusokkal szemben, valamint megakadályozhatjuk a spam feladójának küldött pozitív visszajelzés továbbítását. A kéretlen reklámüzeneteket ugyanis gyakran HTML-formátumban küldik, amely grafikákra történő hivatkozásokat tartalmaz. Amint az automatikus betekintő megnyitja az ilyen e-maileket, és ezzel letölti a grafikákat, a spam küldője visszajelzést kap arról, hogy az e-mail-cím létezik és használatban is van.

Indítsuk el az Outlook Expresst, és válasszuk ki a *Nézet* menüben az *Elrendezés* opciót. A regiszterlap alsó részében távolítsuk el a *Betekintő megjelenítése* előtti kis pipát. Hagyjuk jóvá az *OK* gombbal.

Az Outlookban a *Nézet* menüben található a külön *Betekintő* menüpont, amellyel egyszerű egérgombkattintással megjeleníthető, illetve eltávolítható az ablak.

2.3.2 A Letiltott feladók listájának módosítása

Időről-időre felül kell vizsgálnunk a blokkolt feladók feketelistáját is. Az elavult címeket törölhetjük, a hatástalan bejegyzéseket módosíthatjuk. Az Outlook Express *Eszközök* menüjében kattintsunk az *Üzenetszabá-*



Megadhatók a blokkolni kívánt e-mail-címek

lyok/Letiltott feladók listája opcióra. Jelöljünk ki egy címet, és válasszuk a *Törlés* gombot, hogy törölhessük a bejegyzést. Ha viszont a *Módosítás*-ra klikkelünk, a következő párbeszédablakban felülírhatunk vagy kijavíthatunk egy-egy címet.

2.3.3 Vigyázzunk a domain-blokkolásoknál!

Az utóbbi időben tömegesen terjednek az olyan spam-mailek, amelyeket nemzetközileg ismert szolgáltatók külföldi domainjeiről küldenek el. A kéretlen üzenetek így például Olaszországból a *@lycos.it* vagy Görögországból a *@yahoo.gr* címről is érkezhetnek. Az ilyen mail-domaineket az Outlook Expressben minden további nélkül blokkolhatjuk, ha nem épp olasz vagy görög partnerekkel levelezünk. A hazai címekkel viszont rendkívül óvatosan kell bánnunk, mivel ezzel az eljárással azt kockáztathatjuk, hogy ártalmatlan maileket is blokkolunk.

2.3.4 Feladók tiltása vagy szabályok beállítása?

Ha blokkolunk bizonyos e-mail-címeket vagy -domaineket, akkor bizonyos feladók üzeneteit általánosságban kizárjuk. Az Outlookban és az Outlook Expressben úgynevezett „szabályok" állnak a rendelkezésünkre, hogy a spam-mailek kezelését egzaktabb módon tudjuk definiálni. Ezzel a szűrővel a spam-maileket például színekkel jelölhetjük vagy közvetlenül a kukába továbbíttathatjuk. A szabályok a mindig újabb és újabb feladói címeket használó rafinált spam-küldőkkel szemben is védelmet nyújtanak, ha bizonyos hívószavakat spam-kritériumként adunk meg. Vegyük figyelembe azonban, hogy a szabályok csak az olyan spam-maileknél működnek, amelyek egyértelmű fogalmakat tartalmaznak a tárgysorban, a szövegben vagy a feladói címben.

2.3.5 A szabályok tesztelése

Mielőtt a szűrőszabállyal automatikusan törölnénk bizonyos e-maileket, ellenőrizzük, hogy a kívánt módon működnek-e a szabályok. A spam-mailek esetében az *Áthelyezés a Törölt elemek mappába* akció jó eszköz, mivel a tévesen kiválogatott e-maileket ebből a mappából még visszaszerezhetjük. Természetesen ennek az a feltétele, hogy először deaktiváljuk az *Eszközök/Beállítások/Karbantartás* menüben a *Kilépéskor*

a „Törölt elemek" mappa ürítése beállítást. Ha a szűrőnk kifogástalanul működik, akkor aktiválni tudjuk ezt a beállítást.

2.3.6 Szabályok beállítása az Outlookkal

Ha az Outlookkal dolgozunk, akkor a szűrők beállításánál kicsit másképp kell eljárnunk, mint az Outlook Express esetében. Jelöljük ki az Outlookban a *Beérkezett üzenetek* mappát, és a *Speciális* menüben válasszuk ki a *Szabálykezelő* opciót. A következő párbeszédablakban kattintsunk az *Új* gombra. Válasszuk a *Szabály minta alapján* opciót, és a felső mezőben válasszuk ki például az *Üzenetek továbbítása a tartalomtól függően* opciót.

A párbeszédablak alsó részében kattintsunk a kék aláhúzott változókra, és a beviteli mezőkben adjunk meg olyan hívószavakat, mint például „hot" vagy „money", majd nevezzük meg a „Törölt elemek" mappát mint célmappát. A későbbiekben ezeket az adatokat tovább pontosíthatjuk, és kivételeket is meghatározhatunk. Használjuk mindig a *Tovább* gombot, adjunk a szabálynak egy egyértelmű nevet, és hagyjuk jóvá a *Befejezés* paranccsal.

2.4 Az Outlook XP is segít

Az Outlook XP kínál egy funkciót, amely a spamet még azelőtt blokkolja, mielőtt a nem kívánatos adatszemét a PC-nkre juthatna.

Egy speciális beállítással először csak a mailek fejléceit töltjük le a PC-nkre. Így rögtön láthatjuk, melyik mailt akarjuk valóban fogadni, a gyanús eredetű maileket pedig törölhetjük, és csak a kívánatos levéltartalmakat töltjük le. Ezzel elkerülhetjük, hogy az Outlook-postafiókunkat elöntse a szemét. Ezt a manuális eljárást tovább finomíthatjuk a Levélszemétszűrés szabályvarázslójával és szervezőjével.

2.4.1 A Remotemail telepítése

Ahhoz, hogy élni tudjunk a fejlécek letöltésének a lehetőségével, előbb aktiválnunk kell a *Remotemailt.* A legtöbb telepítőrutin ugyan automatikusan telepíti ezt a funkciót, de a biztonság kedvéért ellenőrizzük még egyszer a beállítást.

Nyissuk meg a *Beérkezett üzeneteket.* Menjünk az *Eszközök* menüre, és húzzuk az egérmutatót a *Küldés/Fogadás beállításai*-ra. A most megjelenő almenüben kattintsunk a *Küldési/Fogadási csoportok megadása* pontra. Megjelenik a *Csoportos küldés/fogadás* ablak.

A *Csoport neve* kiválasztólistán kattintsunk valamelyik csoportra, majd a *Szerkesztésre.*

Kapcsoljuk be a megjelenő ablakban a kiválasztólista mellett a *Levelek fogadása* előtti ellenőrzőnégyzetet. Ezután kattintsunk az OK-ra. Most kövessük az *Offline* mappafájl (OST) elkészítéséhez szükséges, a képernyőn megjelenő utasításokat. Ha a PC-n nem jelennek meg utasítások, akkor a *Remotemail* funkció már telepítve volt.

2.4.2 Alapértelmezések a Beállításokkal

A következőkben leírt beállítás olyan felhasználóknak érdekes, akik következetesen mindig csak a fejléceket szeretnék először letölteni. Ahhoz ugyanis, hogy teljesen szabadon dönthessük el, mit szeretnénk letölteni, be kell tennünk egy saját menüpontot a fejlécek szerkesztéséhez.

Az *Eszközök/Beállítások* menüparanccsal eljutunk az azonos nevű párbeszédablakba. Menjünk ebben az ablakban a *Levelezés beállítása* regiszterlapra.

Itt kattintsunk a *Küldés/Fogadás* gombra. Megjelenik a *Csoportos küldés/Fogadás* ablak. Kattintsunk a *Szerkesztésre.* A most megjelenő ablakban közvetlenül bekapcsolhatjuk a *Csak az elem leírásának a letöltése* lehetőséget. A program ettől kezdve mindig csak a fejléceket fogja letölteni. Olyan kiegészítő lehetőségünk is van, hogy a leírás letöltését csak nagyméretű küldeményeknél választjuk. A méretheatárt egy beviteli mezőben adhatjuk meg.

2.4.3 A fejlécek menüsorának bővítése

A fejlécelemek szerkesztésének kényelmes módja, ha készítünk egy kifejezetten erre a célra szolgáló új menüparancsot. Ennek az új menüparancsnak a segítségével a fejléceket letölthetjük, kiválaszthatjuk és szerkeszthetjük.

Hogy a fejlécek szerkesztéséhez saját menüparancsot készíthessünk, először váltsunk a *Bejövő posta* nézetre. A *Nézet/Eszköztárak* menüben

menjünk a *Testreszabás* parancsra. Megjelenik az azonos nevű ablak. Kattintsunk a *Parancsok* regiszterlapra. A *Kategóriák* listamezőről válasszuk ki az *Eszközök* bejegyzést. A *Parancsok* listamezőt görgessük le addig, amíg eljutunk a *Fejlécek használata* parancsig. Húzzuk ezt a parancsot lenyomott bal egérgombbal a menüsor egy szabad helyére.

2.4.4 Fejlécek fogadása

A fejlécek letöltésével csak a *Tárgy*, *Feladó, Dátum* és *Melléklet* információkat tartalmazó mezők jönnek át. Ez gyorsan megy, és ezekből az adatokból rögtön láthatjuk, hogy melyik levél érdekes, és melyiket lehet mindjárt törölni a szerverről.

Menjünk a *Fejlécek használata* menüparancsra. A most megjelenő almenüben kattintsunk a *Fejlécek letöltése* parancsra.

Most megérkeznek az e-mailjeink fejlécei. Ezen a ponton már megszakíthatjuk az online-kapcsolatot, és nyugodtan átnézhetjük a fogadott leveleket. A legtöbbnél rögtön látjuk, ha spamről van szó.

Mindent, ami spam-mailnek néz ki, vagy valamiért gyanúsnak tűnik, már itt töröljünk. Jelöljük ki ezeket a leveleket. Menjünk a *Fejlécek használata* menüpontra. Az almenüben vigyük az egérmutatót az *Üzenetek megjelölése/Jelölés eltávolítása* parancsra. A most megjelenő almenüben kattintsunk a *Törlés-re.*

2.4.5 A fejlécek feldolgozása

Mindent, ami nem tűnt spamnek vagy gyanús üzenetnek, előkészíthetünk a teljes fogadásra tartalommal és mellékletekkel együtt.

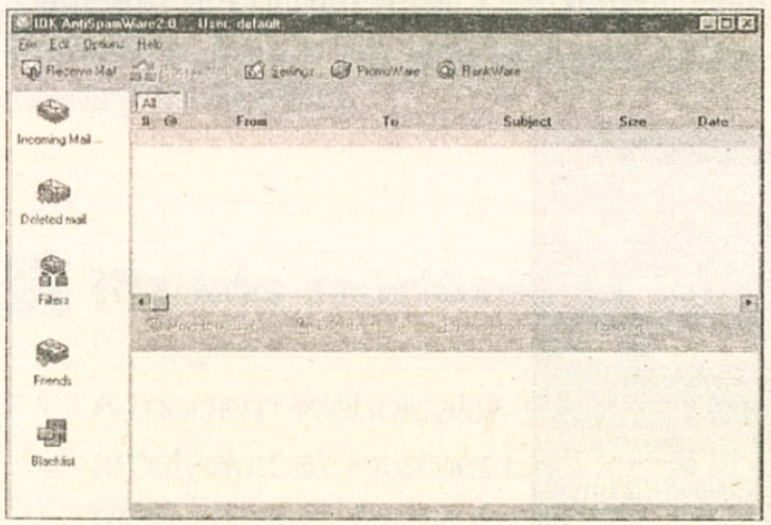
Jelöljük ki azoknak az üzeneteknek a fejlécét, amelyeket kompletten le szeretnénk tölteni. Kattintsunk a *Fejlécek használata* menüparancsra. Az almenüben húzzuk az egérmutatót az *Üzenetek megjelölése/Jelölés eltávolítása* bejegyzésre. A most megjelenő almenüben adjuk ki az *Üzenetek megjelölése letöltésre* parancsot. Ha a kijelölt e-mailekről csak másolatot szeretnénk letölteni úgy, hogy az eredeti a szerveren maradjon, válasszuk az *Üzenet másolatának megjelölése letöltésre* parancsot.

Miután minden fejlécet kijelöltünk és egy feldolgozási művelethez rendeltünk, indulhat a műveletek végrehajtása. Ehhez adjuk ki a *Fejlécek használata* menüben a *Megjelölt fejlécek feldolgozása* parancsot. A tör-

lésre kijelölt maileket a program most törli a szolgáltató mail-szerveréről, anélkül, hogy azok a PC-nkre kerülnének.

2.5 Egy ügyes segédeszköz: az AntiSpamWare

Az Outlook és az Outlook Express szűrőszabályaival kiszűrhetjük a spam-maileket. A szabályvarázslók kezelése azonban egyszerűbb is lehetne, ráadásul a szűrőszabályokkal még semmit sem teszünk a spam-mailek küldői ellen, akik továbbra is elárasztják a postafiókunkat digitális szeméttel. Nos, éppen itt lép be a küzdelembe a CD-mellékletünkön is megtalálható *AntiSpamWare* program, amellyel áttekinthetően, egérkattintással hozhatunk létre és kezelhetünk spam-listákat és szűrőszabályokat. A *panasz funkcióval* egy *ál szerverüzenetet* hoz létre, amely elhiteti a feladóval, hogy a címzett e-mail-címe egyáltalán nem létezik. Az AntiSpamWare-t először azonban gondosan konfigurálni kell.

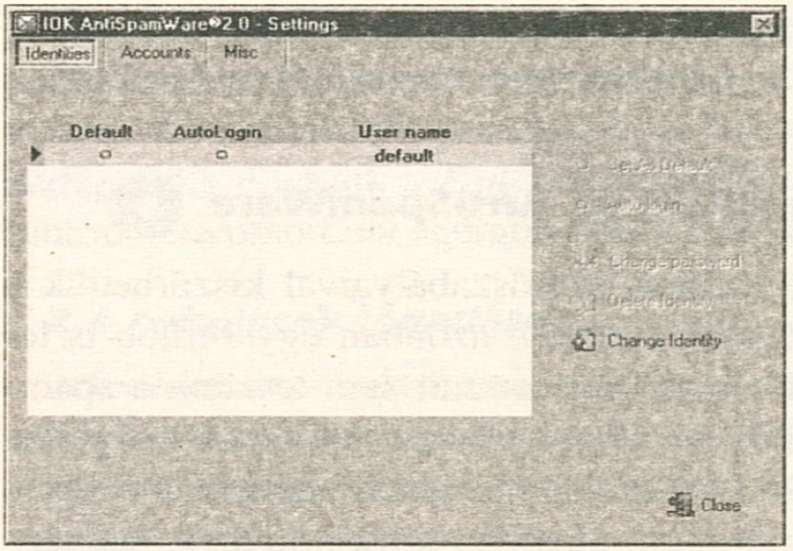


Az AntiSpamWare segítségével könnyen kiszűrhetjük a levélszemetet

2.5.1 Postafiók-beállítások

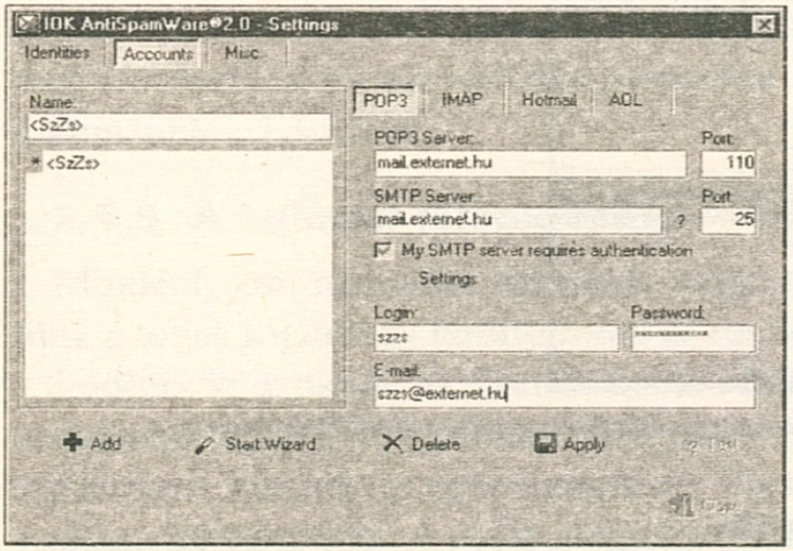
Az AntiSpamWare telepítése után először be kell állítanunk néhány apróságot.

Kattintsunk az eszközsoron a *Beállítások (Settings)* gombra. Ha a számítógépet többen is használják, a *Felhasználói profilok (Identities)* regiszterlapon rendezzük be saját személyes hozzáférésünket, máskülönben az AntiSpamWare az *Auto login* beállítással indul.



Az AntiSpamWare indítása AutoLogin beállítással

Menjünk az *Accounts* regiszterlapra, és a jobb oldalon válasszuk ki, hogy a postafiókunk POP3-, IMAP-, Hotmail- vagy AOL-fiók. Ennek megfelelően írjuk be a kiszolgáló adatait, és a regiszterlap bal oldalán a *Név (Name)* alatt adjunk egyértelmű megnevezést.



Új fiók létrehozása

Menjünk a *Misc* regiszterlapra. A legördülő menüből válasszuk ki a levelezőprogramunkat, és tegyünk pipát a *Levelezőprogram indítása a levelek szerkesztése után (Start mail client after mail processing)* beállítás elé. Állítsuk be, hogy mennyi időnként töltse le automatikusan a leveleket.

2.5.2 Üzenetek szűrése és panaszok küldése

A program önállóan ellenőrzi az új e-maileket, és a megbízható maileket a *Bejövő üzenetek* mappába sorolja. Ezzel szemben a reklám a *Spam* mappában landol.

Legelőször kattintsunk balra fent a *Fogadás (Receive Mail)* gombra. Ezután ellenőrizzük a *Bejövő üzenetek (Incoming mail)* mappában megjelenő bejegyzéseket. Ha spamre akadunk közöttük, kattintsunk a helyi menüben a *Tiltólistára,* hogy az érintett feladótól érkező e-maileket a program törölje a továbbiakban.

Ezzel szemben a megbízható e-mail-címeket felvehetjük a *Barátok (Friends)* listára, hogy ezeknek az üzeneteit a jövőben már ne kelljen ellenőrizni.

Kattintsunk egy kijelölt spam-mail helyi menüjében a *Panasztételre (Complain),* mire kapunk egy három regiszterlapos ablakot. Válasszuk a *Hibaüzenet a feladónak* lehetőséget, hogy a spamküldő egy állítólagos üzenetet kapjon az e-mail szolgáltatónktól arról, hogy az e-mail-címünk ismeretlen. Ez a trükk azonban csak akkor működik, ha a szerverünk támogatja az SMTP-t.

3 Rizikós szörfözés és levelezés

A modern weboldalak sok olyan összetevőt tartalmaznak,
amelyeket az Internet Explorer automatikusan elindít,
még akkor is, ha azok károsak. Ebben a fejezetben bemutatjuk,
hogyan lehet védekezni ez ellen,
és hogy miként tehetjük biztonságossá a levelezésünket.

Szinte mindenkinek van Internet Explorere, és majdnem mindenki az alapértelmezett biztonsági beállításaival internetezik. Ez azonban roppant kockázatos: az Internet Explorer a beleegyezésünk nélkül futtathat olyan alkalmazásokat vagy scripteket, amelyek később károsnak bizonyulnak. Persze az Internet Explorer ettől még nem hiányos felszereltségű. Sőt, át-

fogó biztonsági beállításokat kínál, amelyek más böngészőkhöz viszonyítva példaértékűek. A kezdőknek azonban nehéz áttekinteni, hogy mit is jelentenek egyenként ezek a beállítások. A következőkből kiderül, mely beállításokat kell választanunk, hogy biztonságosan szörfözhessünk az Internet Explorerrel.

3.1 ActiveX – a visszaélés veszélye

Az Internet Explorerben az úgynevezett ActiveX-komponensek jelentik a legnagyobb problémát. Ha ezeket a program bármikor futtathatja, fennáll a veszélye, hogy bizonyos alkalmazások ActiveX-vezérlőelemeken keresztül szereznek elérést a PC-nkre.

Így például néhány új betárcsázó is ActiveX-összetevők segítségével települ fel. Ha túl alacsony fokozatú biztonsági beállításokkal rossz oldalakra tévedünk, automatikusan vagy egy meggondolatlan *Igen* kattintásra feltelepülhet a gépünkre a káros alkalmazás. Ha viszont megtiltjuk az Internet Explorernek, hogy ActiveX-elemeket futtasson, hasznos vagy legalábbis ártalmatlan weboldalakat is gyakran csak korlátozottan nézhetünk meg vagy kezelhetünk.

Ráadásul egyes böngésző-plugin-ek, például a *Flash Player* plug-in a *Macromédiától,* ActiveX-vezérlőkkel működik. Ha letiltjuk az ActiveX-használatot, az Internet Explorer nem tud flash-animációkat megjeleníteni. Az olyan weboldalak, amelyek sok flash-elemmel működnek, nem is fognak megjelenni.

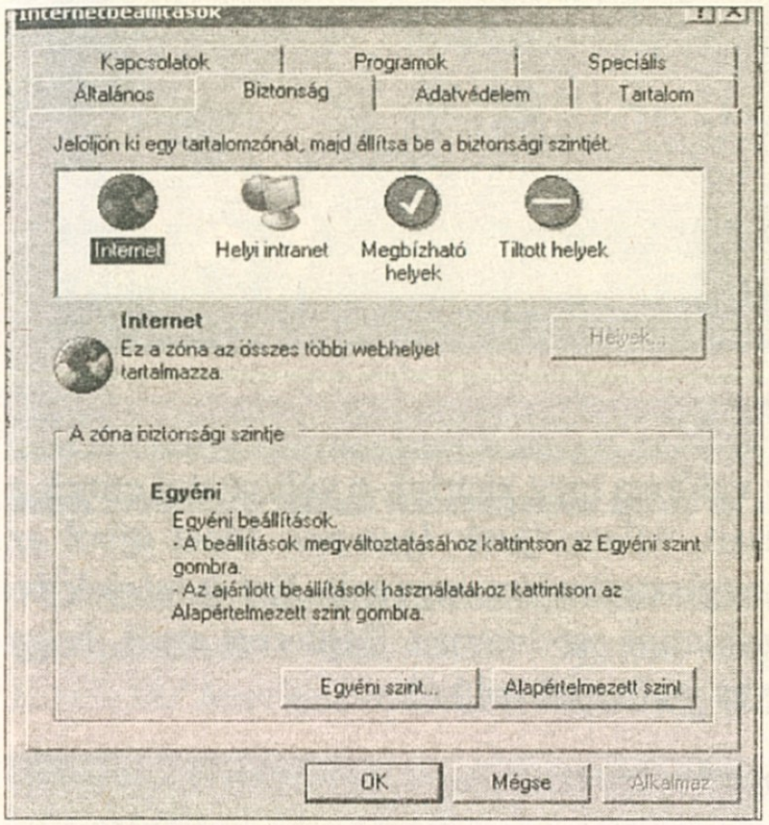
3.1.1 A biztonságos beállítás

A következőkben megmutatjuk, hogyan lehet kordában tartani az ActiveX-elemeket úgy, hogy ennek ellenére kényelmesen mozoghassunk kedvenc weboldalainkon. Ehhez kedvenc weboldalainknak kell szabad utat adnunk, míg más oldalaknál óvatosságra kell intenünk az Internet Explorert.

Először állítsuk be, hogyan járjon el az Internet Explorer a potenciálisan veszélyes weboldalaknál. Alapvetően minden weboldal, amelyet nem emeltünk ki megbízhatóként, potenciálisan veszélyes oldalnak számít.

Nyissuk meg az Internet Explorert, és válasszuk az *Eszközök/Internetbeállítások* menüpontot. Kattintsunk az *Internetbeállítások* ablakban a

Biztonság regiszterlapra. A felső, fehér területen vízszintes görgetősávval négy ikon látható. Ezek négy webtartalomzónát jelölnek, amelyekbe a böngésző beosztja a megjelenített weboldalakat.

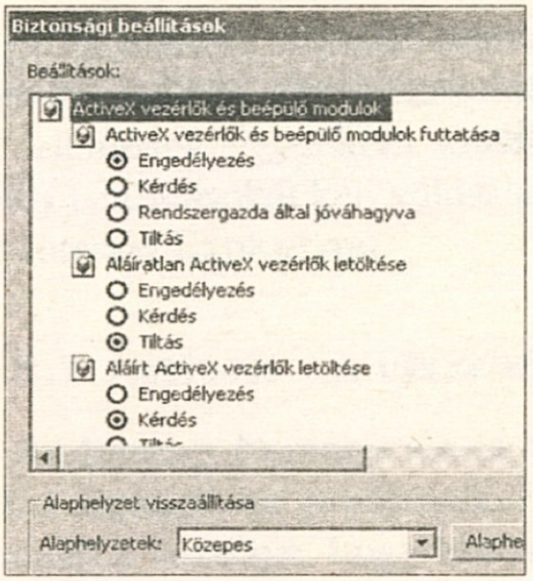


A négy webtartalomzóna

Jelöljük ki az *Internet* tartalomzónát, amelyet a földgolyó jelöl. Győződjünk meg arról, hogy az *Alapértelmezett szint* gomb jobbra lent ki van szürkítve. Ha nincs, kattintsunk rá. Ezután kattintsunk mellette balra az *Egyéni szint...* gombra.

Megnyílik a *Biztonsági beállítások* ablak. Egy hosszú listán fel vannak sorolva azok a beállítások, amelyek a *Közepes* biztonsági beállításhoz tartoznak. Ezeket a biztonságunk érdekében szabjuk testre. Kezdjük az ActiveX-vezérlőkkel! Állítsuk a lista elején mind az öt, ActiveX-re vonatkozó beállítást *Tiltás*-ra.

A jobb oldali gördítősávval görgessük le a listát a *Parancsfájlkezelés* pontig. Itt állítsuk tiltásra a *Beillesztés műveletek engedélyezése parancsfájlokon keresztül* alpontot. Az *Active Scripting* pontot hagyjuk engedélyezve. A változtatásokat hagyjuk jóvá az OK-ra kattintva.



Beállítások a közepes biztonsághoz

A következő kérdésre, hogy valóban meg akarjuk-e változtatni ennek a biztonsági zónának a beállításait, válaszoljunk *Igen-nel.* Most újból az *Internetbeállítások Biztonság* regiszterlapján vagyunk. Ezt is zárjuk be OK-val. Ezzel először is leszoktattuk az Internet Explorert arról, hogy könnyelműen bánjon a veszélyes webtartalmakkal.

3.1.2 A Megbízható zóna testreszabása

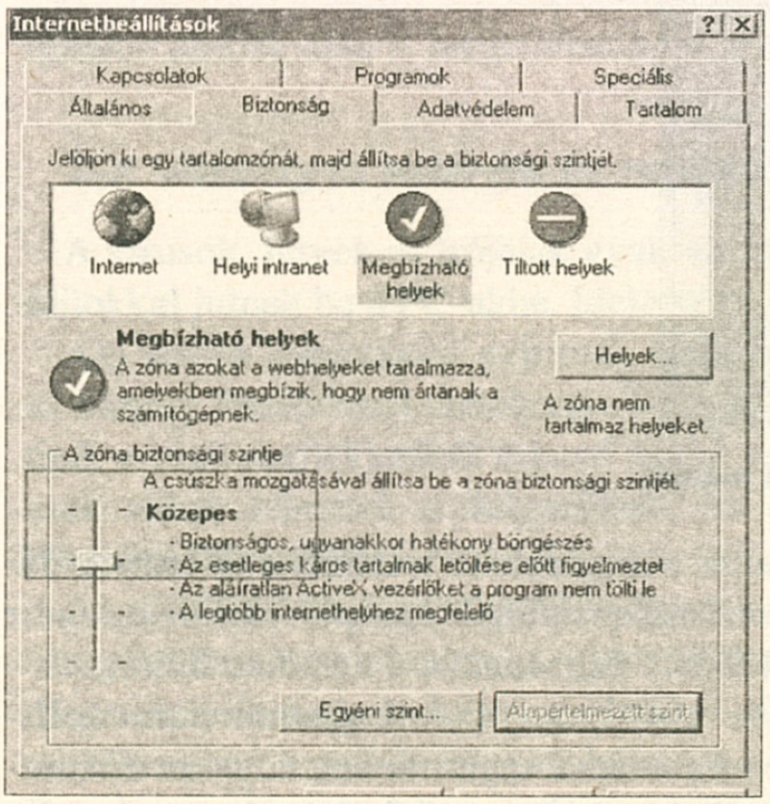
Az Internet Explorer minden weboldallal azok szerint a beállítások szerint jár el, amelyeket az imént az Internet tartalomzónához beállítottunk. A probléma: így az olyan webtartalmakat sem tudjuk rendesen megjeleníttetni, amelyekben megbízunk, és amelyek hasznos ActiveX-elemekkel működnek.

Ha például a flash animációkkal művészien megtervezettt **www.kunst-museum-wolfsburg.de** oldalon szörfözünk, az Internet Explorer azt az üzenetet küldi, hogy az oldalt nem tudja megjeleníteni.

Bizonyos oldalakat OK-val való tudomásvétel után ugyan megnézhetünk, a múzeum esetében azonban a weboldal ActiveX-támogatás nélkül üres marad. A böngészőnek ugyanis szüksége van egy flash plug-in-re egy ActiveX-elem formájában. A problémát úgy oldhatjuk meg, ha az oldalt egy másik zónához rendeljük. Azokat az oldalakat, amelyeknek bizalmat szavazunk, a *Megbízható helyek* közé sorolhatjuk az Internet Explorerben.

Flash animációk nélkül élvezhetetlen lenne ez a weboldal

De mielőtt megkezdenénk a hozzárendelést, szabjuk testre ennek a tartalomzónának a beállításait! Nyissuk meg az Internet Explorerben az *Eszközök/ Internetbeállítások/Biztonság* ablakot. Jelöljük ki a *Megbízha-*



A „közepes" biztonsági fokozat már némi elővigyázatosságra utal

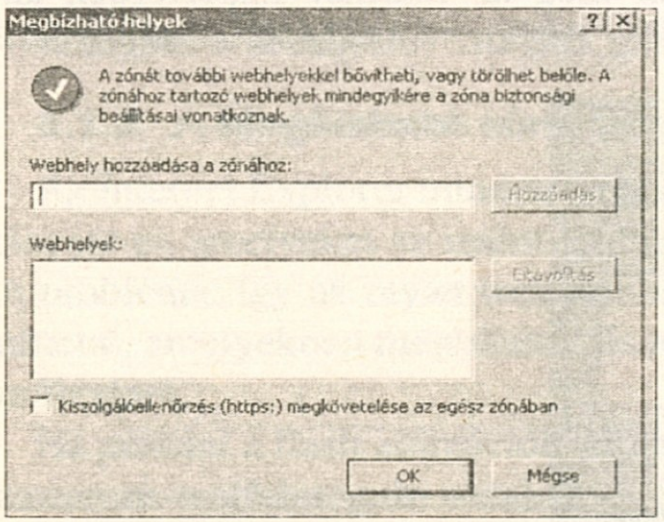
tó helyek zónát, amelyet zöld körben pipa jelöl. Az ablakban balra lent megjelenik egy csúszka, amely a *Nagyon alacsony* szintre van beállítva.

Még a megbízható weboldalaknál is legyünk óvatosak. Ezért húzzuk a csúszkát lenyomott bal egérgombbal két fokozattal feljebb, a *Közepes* biztonsági fokozatra. Ezen a fokozaton, amely az internetes tartalomzóna alapértelmezése, majdnem minden weboldalt meg tudunk nézni – legyen az ActiveX-szel vagy anélkül. Ezt a luxust azonban csak a megbízható weboldalaknál engedjük meg magunknak. A beállításokat az *Alkalmaz* gombbal hagyjuk jóvá.

3.1.3 Megbízható weboldalak bejegyzése

Az olyan weboldalt, amelyben megbízunk, azonban az ActiveX-elemek vagy a plug-in-ek miatt csak korlátozott formában jelenik meg, vegyük fel a *Megbízható helyek* közé.

Még mindig az *Internetbeállítások/Biztonság* ablakban vagyunk, a zöld zónajel a fehér pipával van kijelölve. Kattintsunk a *Helyek...* gombra.



Bővíthetjük a megbízható helyek listáját

A következő ablakban kezeljük a megbízható webhelyeink címeit. Távolítsuk el a pipát a *Kiszolgálóellenőrzés (https:) megkövetelése az egész zónában* beállítás elől, és a *Webhely hozzáadása a zónához* felirat alá – példánknál maradva – írjuk be elsőként a **www.kunstmuseum-wolfsburg.de** címet. Az Internet Explorer azzal segít minket, hogy az *Előzményekből* legördülő listán felkínálja kiválasztásra a webcímeket.

Mellette jobbra kattintsunk a *Hozzáadás* gombra, és a cím bekerül a *Webhelyek* mezőbe. Adjunk két OK-t, és ellenőrizzük az imént készült bejegyzést. Hívjuk be ismét a művészeti múzeum webcímét. Az Internet Explorer zokszó nélkül behozza az oldalt. Figyeljünk jobbra lent az állapotsoron megjelenő zónaikonra. Most éppen a *Megbízható helyek* jelenik meg, mivel a weboldal ezek közé tartozik.

3.1.4 Gyorsabb hozzáadás

Most keressünk fel egy másik weboldalt, amelynek bizalmat szavazunk, például az internetbankunkat vagy egy online folyóiratot. Jobbra lent az állapotsoron ismét az *Internet* zónaikon jelenik meg, mivel ezt az oldalt eddig még nem soroltuk be a megbízhatóak közé.

Kattintsunk duplán a lenti kis zónaikonra – és rögtön megjelenik a biztonsági zónák ablaka. Jelöljük ki a *Megbízható helyeket,* és a *Helyek...* gombbal nyissuk meg a webcímlistánkat. Az eljárás megegyezik az előző pontban leírttal.

Figyelem! A teljes webcím helyett mindig csak az oldal domain-nevét írjuk be. A **http://www.atec-diving.com/index.html/stb.** helyett elegendő egyszerűen a főcím **www.atec-diving.com.** Ezután ennek az oldalnak minden alkönyvtára is megbízhatóként lesz beosztva.

3.2 Veszélyes mail-ek és letöltések

A vírusok, férgek és trójaiak gyakran levélmellékletként vagy letöltött fájlokkal jutnak be a PC-nkbe. Ideje véget vetnünk ennek.

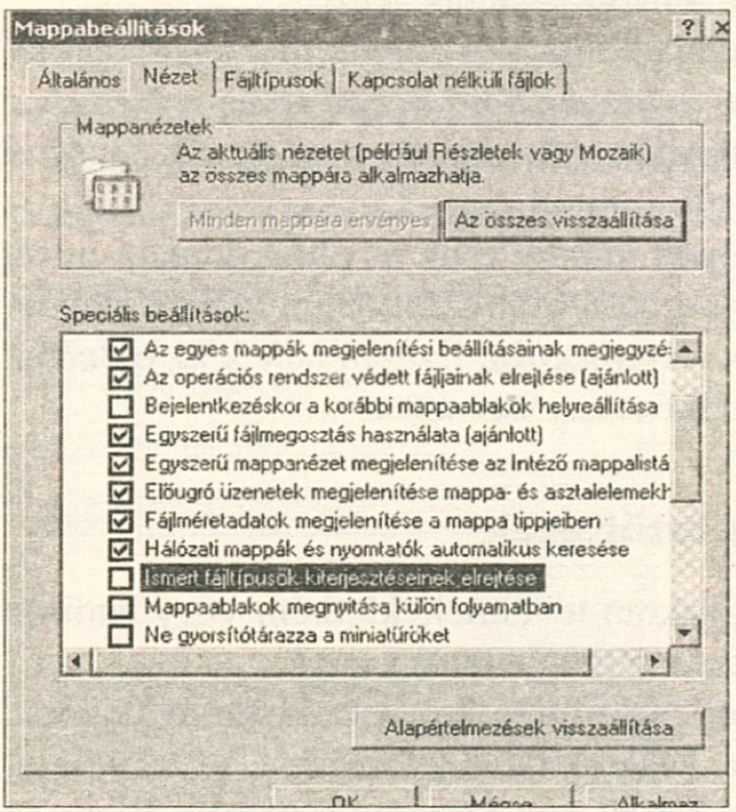
Aki kettős kattintással nyit meg ismeretlen helyről származó fájlokat, az bizony felelőtlenül cselekszik. Még az ismert forrásból, pl. egy barátunk e-mail-mellékletéből érkező fájlok sem feltétlenül tiszták. Biztosak csak akkor lehetünk a dolgunkban, ha egy aktualizált víruskeresővel megnézettük a fájlt.

Az alábbiakból megtudhatják, hogyan kell a Windows alatt a letöltések vizsgálatához megjeleníteni a rejtett fájlkiterjesztéseket. Ezen kívül azt is megmutatjuk, hogyan lehet az Outlook Express levelezőprogramot biztonságosabbá tenni, és hogyan lehet az *AntiVir* víruskeresővel dolgozni. Ennek a magáncélú felhasználása ugyanis ingyenes.

3.2.1 A fájlkiterjesztések ellenőrzése

A Windows alapbeállítása szerint az ismert fájltípusok kiterjesztését elrejti. A felhasználó így az „.exe", „.com" vagy „.vbs" kiterjesztésű fájlokat, és a „.txt", „.jpg" vagy „.gif" kiterjesztésű kép- vagy szövegfájlokat nem képes megkülönböztetni egymástól. Az előbbiek tartalmazhatnak veszélyes kódokat, az utóbbiak nem. Ezért gondoskodjunk arról, hogy a Windows megjelenítse a kiterjesztéseket.

Nyissuk meg a Windows XP alatt a *Start/Vezérlőpult* menüben a *Mappa beállításai-t,* és válasszuk a *Nézet* regiszterlapot. A *Speciális beállítások* listájában távolítsuk el az *Ismert fájltípusok kiterjesztéseinek elrejtése* opció kijelölését. Az *OK*-val nyugtázva lépjünk ki ebből az ablakból.



Láthatóvá tehetjük a fájltípusok kiterjesztését

A Windows 98 alatt a *Start/Beállítások* menüben találjuk a *Mappa beállításait.* Válasszuk ki itt is a *Nézet* regiszterlapot, és távolítsuk el az *Ismert fájltípusok kiterjesztéseinek elrejtése* opció kijelölését. Az *OK*-val történt nyugtázást követően a Windows a kiterjesztésükkel együtt fogja megjeleníteni a fájlokat.

Alapvető, hogy az internetről letöltött állományokatt – és ez mindenekelőtt a cserebörzékre érvényes – ellenőrizzünk egy aktuális víruskeresővel.

3.3 Biztonságosabb e-mail

Ha a *Küldés* gombra kattintunk az e-mailjeinknél, már nem gondolhatjuk meg magunkat. De az elküldés csak a kezdet a levél életében, hiszen a címzetthez számtalan szerveren keresztül vezet az út. Az üzenetet az út számos pontján elfoghatják, elolvashatják, lemásolhatják vagy meghamisíthatják. Az üzenetünk ki van téve a hackereknek, vírusoknak, trójaiaknak vagy a komputerférgeknek. És amikor az üzenet megérkezik a címzett postaládájába, lehet, hogy nem is az üzenetben megjelölt feladótól jött.

Az e-mailek küldése és fogadása a legtöbb ember számára természetessé vált. Az e-mailekhez való hétköznapi hozzáállás miatt ez az ügyes eszköz a vírusok terjesztésének egyik legegyszerűbb módja. Az olyan széleskörűen használt futtatható csatolt állományok, mint a videók, a rajzfilmek, illetve az egyéb multimédiás programok és animált üdvözlő kártyák, megkönnyítették a károkozó vírusok e-mailes terjedését.

3.3.1 Védjük magunkat!

Legyünk tisztában a tényekkel. Jóllehet, az e-mail az egyik módja a megfertőződésnek, pusztán egy e-mail elolvasásával nem lehet a vírust megkapni. A vírusokat *futtatható csatolt állományokként* terjesztik, és ezt meg kell nyitni ahhoz, hogy megfertőzze a számítógépet. A végrehajtható csatolt állomány egy program, amelyet futtatni kell ahhoz, hogy a vírust megkapjuk. Ha egy vírus, vagy más kártékony program a gépünkre kerül, az átnevezheti vagy törölheti a fájljainkat, névjegyalbumunk segítségével akaratlanul is elküldhetjük a vírust barátainknak vagy kollégáinknak, vagy olyan rések keletkezhetnek a rendszerünkön, amelyen keresztül a hackerek a későbbiekben beléphetnek, és teljes hozzáférést szereznek a számítógéphez.

Legyünk gyanakvóak. Még ha látszólag a legjobb barátunktól kaptuk is a levelet, az tartalmazhat rosszindulatú kódokat. Ha a barátunk e-mailben

vagy az interneten keresztül trójai vírust kapott, az elrejtőzik a számítógépén, és a levelezőprogram segítségével terjeszkedni próbál. Az *I Love You* vírushoz hasonló trójai vírusok gyakran terjeszkednek azáltal, hogy a névjegyalbumban található összes címre másolatot küldenek magukról. A levél látszólag egy megbízható baráttól jött, azonban valójában egy veszélyes trójai vírust tartalmaz, amely a csatolt állomány futtatásával megfertőzi a számítógépét. Annak érdekében, hogy biztonságban legyünk, ellenőrizzünk minden csatolt fájlt, még ha a legbiztosabb forrásból is kaptuk. Ha nem megbízható forrásból jött, bölcsebb egyáltalán nem megnyitni őket.

Használjunk antivírus szoftvert! A vírusok, trójai vírusok és férgek észlelésének egyik leghatékonyabb módszere a megfelelő antivírus szoftver használata, még az esetleges fertőzés előtt. A *Norton AntiVirus* az összes beérkező levelet átvizsgálja fertőzött állományokat keresve, és jelzi azt, ha ilyet talál. A Norton AntiVirus használatával a vírusnak esélyt sem adunk a támadásra. Sőt, e díjnyertes szoftvernek Live Update funkciója is van, s ha a felhasználó online kapcsolatban van, folyamatosan új vírusdefiníciók után kutat, naprakész védelmet garantálva a pusztító programok ellen. A Norton AntiVirus egyszerűen telepíthető, konfigurálható és használható, észrevétlenül fut a háttérben, így soha nem kell aggódnia a bejövő üzenetek postaládát fenyegető veszélyei miatt.

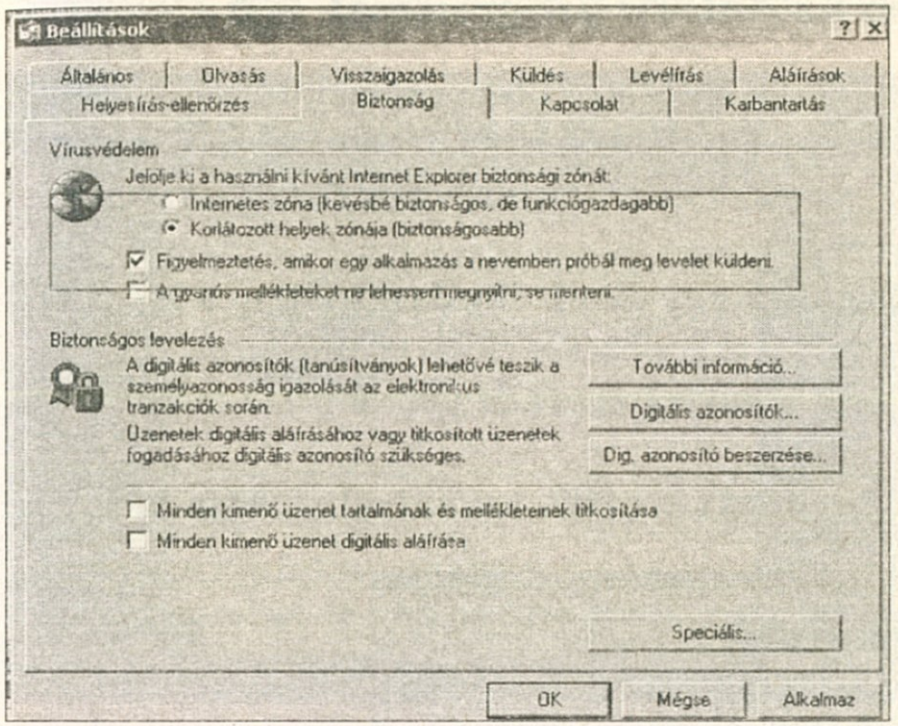
Használjunk személyi tűzfalat! A személyi tűzfal szoftver remek módszer az egész számítógép biztonságossá tételére. A tűzfal az összes bejövő és kimenő információt vizsgálja, számos előre meghatározott biztonsági kritérium alapján. A *Norton Personal Firewall* például azelőtt kapja el a bejövő vírusokat, trójai vírusokat, férgeket és az ActiveX kontrollokhoz és JavaScripthez hasonló veszélyes kódokat, mielőtt azok károsíthatnák a rendszert.

*A személyi tűzfalakról az 5.*fejezetben további részleteket is olvashatnak.

3.4 Az Outlook Express biztonságosabbá tétele

Az Outlook Express 6 már alapértelmezése alapján is rendelkezik némi védelemmel a káros tartalmú HTML mail-ek ellen. Standard beállítása alapján valamennyi HTML formátumú levelet a *Korlátozott oldalak* közé

sorol. Ennek az az előnye, hogy elnyomja az esetleges károsító ActiveX elemeket vagy scripteket, amelyek már a mail megtekintésekor lefuthatnak. Ellenőrizzük ezeket a beállításokat!



Fontos, hogy a képen kiemelt két opciót kijelöljük

Nyissuk meg az Outlook Express-t, és válasszuk ki az *Eszközök/Beállítások* menüben a *Biztonság* regiszterlapot. Itt a vírusvédelem bekezdésben a *Korlátozott helyek zónája (biztonságosabb)* opciónak kijelölve kell lennie. Közvetlenül alatta a *Figyelmeztetés, amikor egy alkalmazás a nevemben próbál meg levelet küldeni* opciót szintén hagyjuk kijelölve. Így az Outlook Express közölni fogja, ha egy alkalmazás titokban a nevünket feladóként használva próbál egy levelet kiküldeni.

Haszontalan viszont a *Gyanús mellékleteket ne lehessen megnyitni se menteni* opció. Ha ugyanis ezt is bekapcsoljuk, akkor az Outlook Express minden levél mellékletéből a megkérdezésünk nélkül eltávolítja az összes futtatható fájlt. Viszont az esetleg makróvírusokat tartalmazó Office-fájlokat minden korlátozás nélkül békén hagyja. Jobb tehát, ha nem jelöljük ki ezt az opciót.

Sose nyissunk meg mellékletet kettős kattintással, közvetlenül a levélből. Kivéve, ha a víruskeresőnk már az érkezésükkor végignézte a levele-

ket. Előbb tároljuk el a mellékletet a *Lemezre mentés* opcióval a merevlemezre, és nézessük meg a víruskeresőnkkel.

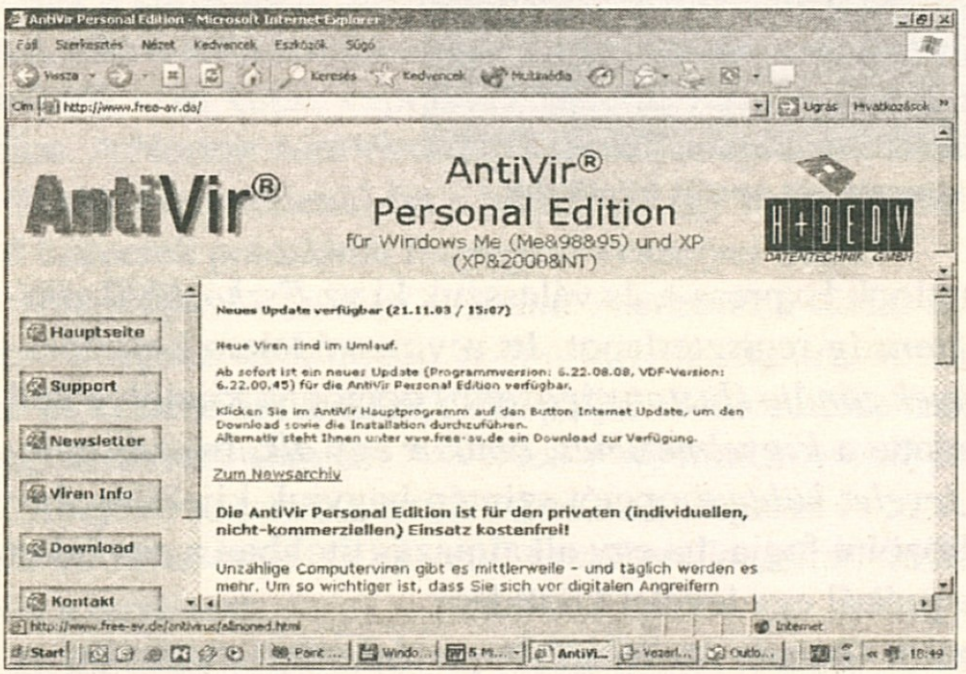
3.5 Vírusvédelem az AntiVir programmal

Ha az internetről töltünk le fájlokat, akkor feltétlenül víruskeresővel kell védenünk a PC-nket. A következőkben a *H+BEDV* által készített *AntiVir* program kezelését ismertetjük, amely magáncélú alkalmazás esetén ingyenes.

Figyelem! Ha a PC-nken van egy másik víruskereső vagy a H+BEDV program egy korábbi verziója, akkor ezeket előbb távolítsuk el.

Töltsük le a víruskeresőt a **www.free-av.de** címről a *Download* rovat alól, vagy CD-mellékletünkről.

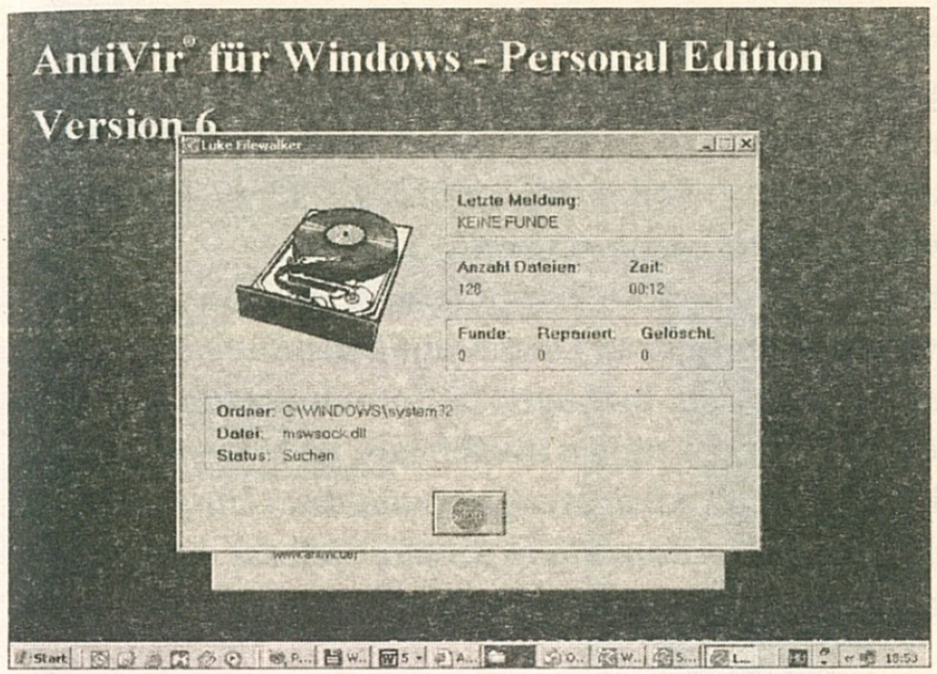
Miután elindítottuk az *avwinsfx.exe* fájlt, kattintsunk a *Setup*-ra és két-



Itt „lakik" az ingyenes antivirus program

szer a *Tovább*-ra. Olvassuk el a licencszerződést, jelöljük ki a *Valamennyi feltétellel egyetértek...(Ich stimme...)* opciót, és háromszor nyomjuk le a *Tovább* gombot, anélkül, hogy változtatnánk az alapértelmezett beállításokon.

A következő megjegyzést *OK*-val nyugtázzuk. A telepítést és a *Tovább (Weiter)* gomb kétszeri megnyomását követően egy Windows-Editorban megjelenik a *Readme* fájl. Ez többek között egy support-fórum címét is tartalmazza, ahol a felhasználók eszmét cserélhetnek.



Munkában az AntiVir

Zárjuk be a tesztablakot, és a *Befejezés* gombra kattintással fejezzük be a telepítést. Az AntiVir most automatikusan végignézi a PC-nket, ismert vírusok után kutatva. A merevlemezen lévő fájljaink számától függően ez egy ideig eltarthat.

3.5.1 A víruskereső beállítása

Az AntiVir két modulból épül fel, a főprogramból és az őrből. Az őr, vagyis a *Guard* a PC minden indulásakor automatikusan betöltődik. Ez munka közben figyeli a PC-t, ezért legyen mindig bekapcsolt állapotban.

A Tálca jobb alsó szélén, a rendszeridő mellett, a nyitott piros esernyő jelzi, hogy az őr aktív. De csak azokat a fájlokat figyeli, amelyeket éppen használunk. Ahhoz, hogy a teljes PC-nket ellenőrizze, amire célszerű legalább kéthetente időt keríteni, a második komponenst, az AntiVir főprogramot is meg kell nyitni.

Nyitott piros esernyő jelzi, hogy az „Őr" nem lustálkodik

Válasszuk a *Start/Minden program* menüben az *AntiVir Personal Edition/AntiVir* bejegyzést. Egy rendszertesztet követően a PC valamennyi meghajtóját láthatjuk. Itt jelöljük ki őket a kereséshez. Mielőtt a keresést elindítanánk, két beállítást kell elvégeznünk az *Opciók/Konfigurációs menüben (Optionen/Konfigurationsmenü)*.

A bal oldali listában jelöljük ki a *Keresést (Suchen)*, és a jobb oldalon a *Fájlok (Dateien)* rovatban jelöljük ki az *Összes fájl (Alle Dateien)* opciót. Ennek hatására az AntiVir nemcsak bizonyos fájlformátumokat fog megvizsgálni, hanem az összes fájlt. Ez ugyan tovább tart, de biztonságosabb.

Ezután válasszuk ki balra a *Nemkívánatos programokat (Unterwünsche Programme)*, és jelöljük ki a *Backdore kliens szoftver jelzése* opciót. *OK*-val nyugtázzunk, és a nagyítóra kattintva indítsuk el a keresést.

3.5.2 Vészjelzések és update-ek

Az internetről ettől kezdve letöltött valamennyi fájlt a merevlemez egy külön mappájába tegyük. Legyen ez például a *D:\Új letöltések* mappa.

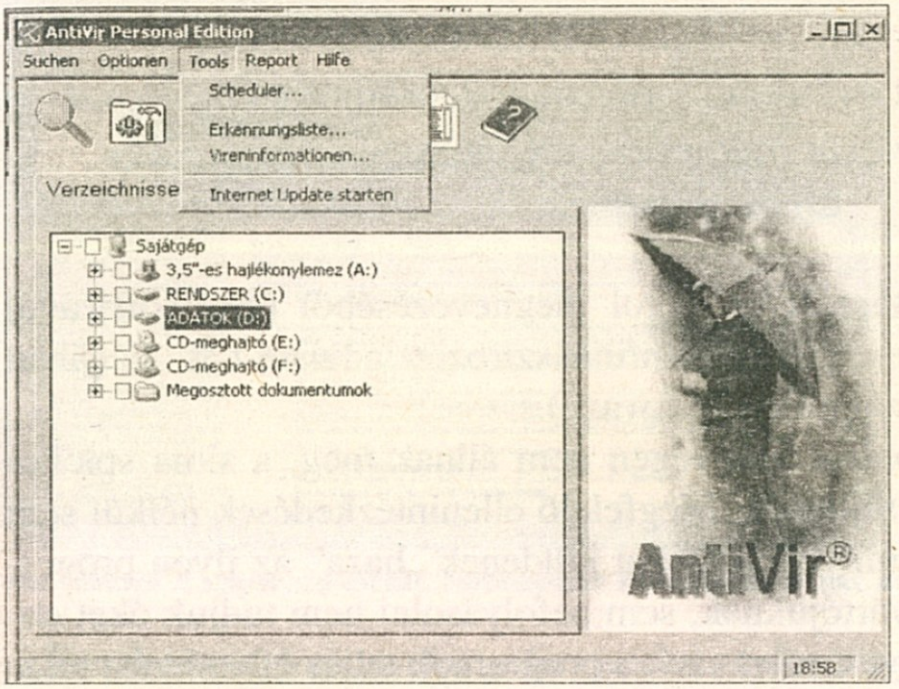
Ugyanez vonatkozik az e-mail-mellékletekre is. A nyitott mail-ben kattintsunk az egér jobb oldali gombjával a mellékletre, és válasszuk a *Mentés másként* parancsot. Ahhoz, hogy a levél tartalmát meg tudjuk vizsgáltatni az AntiVir-rel, kattintsunk rá (ismét a jobb egérgombbal), és a helyi menüből válasszuk a *Víruskeresés AntiVir*-rel *(Virensuche mit AntiVir)* opciót.

Ha az AntiVir gyanús fájlra bukkan, akkor megjelenik a *Figyelmezetés – gyanús fájlt találtam! (Warnung – verdächtige Datei gefunden)* ablak, és figyelmeztető hangot is fogunk hallani. Ha fertőzött fájlról van szó, például egy makróvírusos Word-fájlról, akkor ezt az AntiVir ideális esetben ki tudja javítani.

Figyeljük meg a felső ablakban álló figyelmeztetést. Ha a fájlt nem lehet kijavítani, akkor a következő három lehetőség egyikét kell választanunk. A *Hozzáférés megengedése és a fájl meghagyása (Zugriff erlauben*

und Datei belassen) opciót csak akkor válasszuk, ha biztosak vagyunk benne, hogy nem vírusról van szó.

A víruskereső programok néha vaklármát csapnak. Ekkor segíthet, ha bekukkantunk az AntiVir Support-fórumba vagy a szoftver gyártójának honlapjára. Az AntiVir következő update-jével rendszerint meg is szüntetik a vaklárma okát.



Innen indíthatjuk az update-et

Az AntiVir update funkcióját hetente egyszer használjuk, mert rendszeres frissítés hiányában egyetlen víruskereső szoftver sem képes megvédeni az új vírusoktól. Indítsuk el az AntiVir főprogramját – ne az őrt – az Asztalon található ikonnal, és válasszuk a *Tools/Internet update start* parancsot. Létesítsünk kapcsolatot az internettel, és kattintsunk a *Start* kapcsolóra. Ha nincs új telepítőfájl, akkor *Nem*-mel *(Nein)* nyugtázzunk, és lépjünk ki a *Befejezéssel (Beenden)* az Internet-Update-ből.

Az új AntiVir update rendszerint kéthetes időközönként szokott rendelkezésre állni. Ehhez azonban a teljes telepítőfájlt le kell töltenünk, és újra kell telepítenünk az AntiVir-t. Ehhez lépjünk ki az *Őr*-ből. Kattintsunk az egér jobb oldali gombjával jobbra lent az esernyő ikonra, és válasszuk a *Kontrollprogram bezárását (Kontrollprogramm schließen)*. Ezután folytassuk az update-et, és köves sük az utasításokat.

TiPP PLUSZ

4 Vessünk véget a kémkedésnek!

Emlékszik még rá, milyen weboldalakat látogatott meg az elmúlt hónapokban? Ha nem, kérdezzen rá egyszerűen a spyware-ek gyártóinál – ők garantáltan utána tudnak nézni. Pontosan ez a céljuk és az értelmük ezeknek a programoknak: mindig az a fő, hogy adatokat gyűjtsenek, kikémleljék internetezési és bevásárlási szokásainkat, személyes profilokat készítsenek vagy akár még ennél többet is.

Nem véletlen a kémszoftver angol megnevezéséből (**spy** soft**ware**) származó rövidítés, amely a reklámfinanszírozott adware-t is magában foglalja (**Ad**vertising supported Soft**ware**).

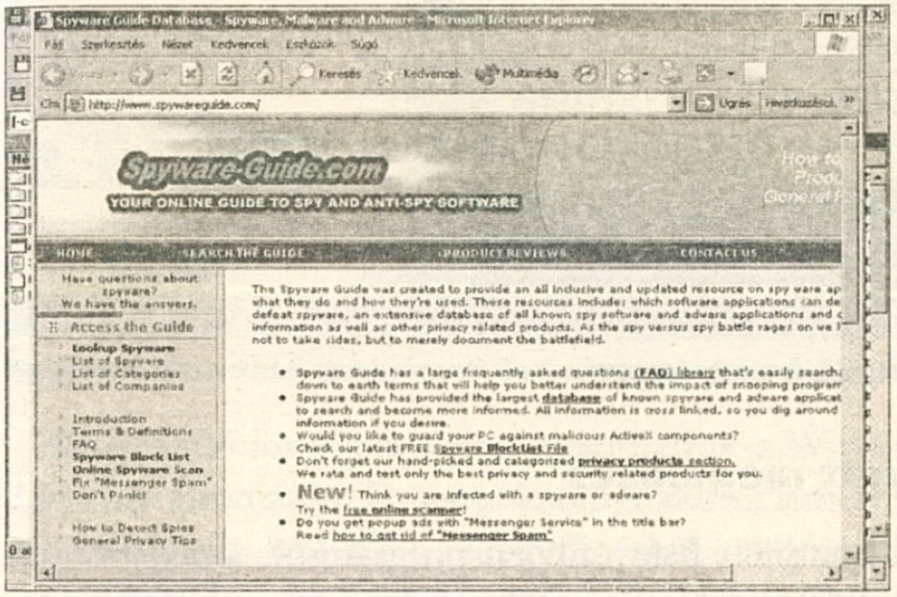
A szaglászásnál azonban már régen nem állnak meg, a sima spiclickedés kereteit messze túllépték. Megfelelő ellenintézkedések nélkül sem azt nem tudjuk, hogy milyen adatokat küldenek „haza" az ilyen programok rendszeresen a gyártójuknak, sem befolyásolni nem tudjuk őket ebben. Ez azért is veszélyes, mert ezek a programok teljes ellenőrzést tesznek lehetővé a számítógépünk fölött. Ezen a módon terjednek még a keyloggerek is, amelyek feljegyzik a billentyűzet-leütéseinket, majd könnyen el tudják küldeni a jelszavakat vagy akár a hitelkártya-számunkat is, amelyet például online-vásárláskor írunk be.

4.1 Sokkal elterjedtebb, mint gondoljuk

Most azt gondolják, mindez Önöket nem érinti? Akkor valószínűleg tévednek. Egyedül az a tény, hogy az egész szaglászásból eddig semmit nem észlelt, senkit sem ringathat biztonságba. Legkésőbb a megmagyarázhatatlan letöltésekre vagy szokatlanul nagy processzor-kihasználtságra kell felfigyelnünk.

A Spyware-Guide (**www.spywareguide.com**) kereken 250 különböző spyware-programot sorol fel. Ennél a számnál csak a különböző spyware-összetevőkről és -cégekről van szó. Az alkalmazások száma, ame-

lyekbe ilyen kémprogramok vannak integrálva, ennek a sokszorosa. Egyedül a *Cydoor* ismert komponensei kerek 2 000 programban rejtőznek. És hogy azt is tudjuk, hogyan kerülnek ezek a programok a PC-nkre: teljesen átlagos szoftverekbe vannak integrálva, amelyeknek a telepítésekor egyszerűen velük együtt települnek fel a számítógépre.

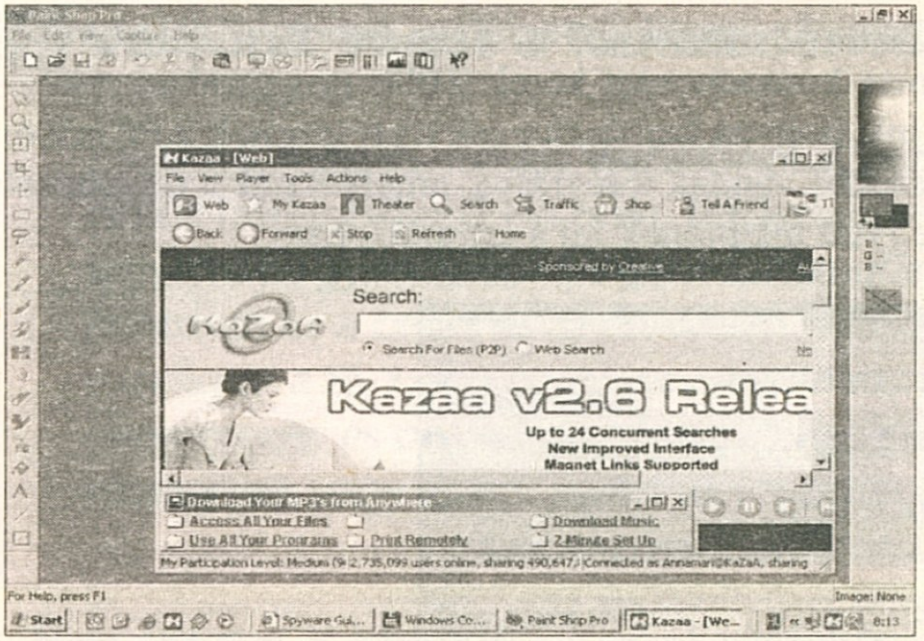


Ha félünk a spyware-ektől, feltétlenül keressük fel ezt az oldalt

Ennek is megvan az oka: a freeware és a shareware programok szerzőit azért fizetik, hogy továbbadják a kívánt felhasználói adatokat a kémvállatoknak. Most már bizonyára szeretnék tudni, hogy milyen programokról van szó! Nos, az alkalmazások listája, amelyek adatokat küldenek haza, végtelen: a Kazaa cserebörze programjai, az ICQ Messenger, a GetRight download-manager vagy az Eudora levelezőprogram csak néhány példa.

Ezzel talán világossá is vált, hogy a spyware problémája sokkal elterjedtebb, mint azt a legtöbb PC-felhasználó gondolná. Ezért is ajánljuk: előzzük meg úgy a bajt, hogy egyáltalán ne telepítsünk fel a számítógépünkre spyware-es felhasználásokat, az újak ellen pedig védekezzünk. Nemsokára az is kiderül, hol tudhatjuk meg, milyen programok működnek spyware-rel vagy adware-rel.

Ezen felül távolítsunk el azokat a kémösszetevőket is, amelyek már működnek és szorgalmasan gyűjtik az adatokat a gépünkön.



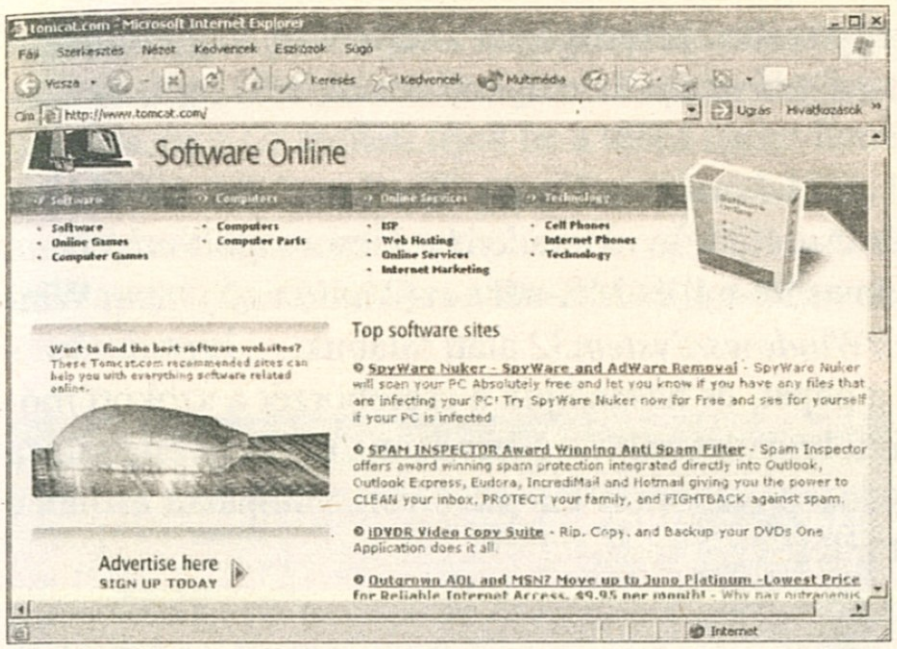
Legyünk óvatosak, ha a Kazaa-t használjuk

4.2 Kivárás helyett megelőzés

Aktuális és ráadásul komplett lista minden programról, amelyek spyware-t vagy adware-t tartalmaznak, nem található az interneten. Jó kiindulópont viszont a **www.cyberspalace.de/htm/sicher1.htm** és a **www.tomcat.com/spybase/index.html** cím. A *TomCat* oldalon vagy egy bizonyos program kezdőbetűire kattintunk, hogy utánanézzünk, hogy az illető alkalmazás fertőzött-e, vagy beírjuk a programnevet közvetlenül a *View Database by Software Name* mezőbe, és *Submit*-tel elindítjuk az ellenőrzést.

Az eredményt a TomCat a *Search Results* alatt listázza ki, ahol egyetlen kattintással további információkat kaphatunk az integrált szimatprogramok fajtájáról vagy sajátosságairól.

Jól tesszük, ha minden új freeware vagy shareware telepítésekor figyelünk a spyware-összetevőkre utaló jelekre. Ezek természetüknél fogva jól el vannak rejtve, vagy csak a végfelhasználói licencszerződés – angolul End User License Agreement, rövidítve EULA – tartalmazza őket. Olvassuk át figyelmesen a feltételeket. Kijelölhetjük például az egérrel a teljes tartalmat, a Windows vágólapjára helyezzük, és a szövegszerkesztőnkbe másoljuk. Így nemcsak kényelmesebb elolvasni, hanem olyan fogalmakat is kereshetünk, mint az *advertis*, *third party*, *banner* vagy mondjuk a *value*.



Spyware-eltávolító programok és hasznos információk egy helyen

Kiegészítő intézkedésként telepíthetjük a Windowsra a *Spyware Block List File* állományt. Ez megakadályozza az ismert spyware-ek és adware-ek telepítését ActiveX-vezérlőről, tehát a hálón való szörfözéskor. Amint egy weboldal megkísérel erről a listáról telepíteni vagy használni egy összetevőt, a program megakadályozza ezt.

Írjuk be az Internet Explorerbe: **www.spywareguide.com/blocklist.reg,** és töltsük le a fájlt a következő ablakban a *Mentésre* kattintva. Ezután dupla kattintással beágyazzuk a „reg"-fájlt a Windowsba, *Igen/OK*-val jóvá hagyjuk, és újraindítjuk a gépet.

4.3 Amikor nem működik

Egyes programokat olyan okosan programoztak, hogy az integrált „szaglászfunkció" nélkül nem, vagy nem teljes értékűen működnek. Mit tegyünk hát, ha szeretnénk a szoftvert megfigyelés nélkül továbbra is használni? Ha ezt a licencfeltételek megengedik, egyszerűen cseréljük le a megfigyelésért felelős fájlt: például a Cydoor kémösszetevős programok a Windows rendszerkönyvtárában található *cd_client.dll*-re épülnek. Ha ezt a fájlt egyszerűen töröljük, akkor a Kazaa vagy a Grokster fájlmegosztó programok nem működnek tovább. Ilyen esetekben ki kell cserélnünk a fájlt.

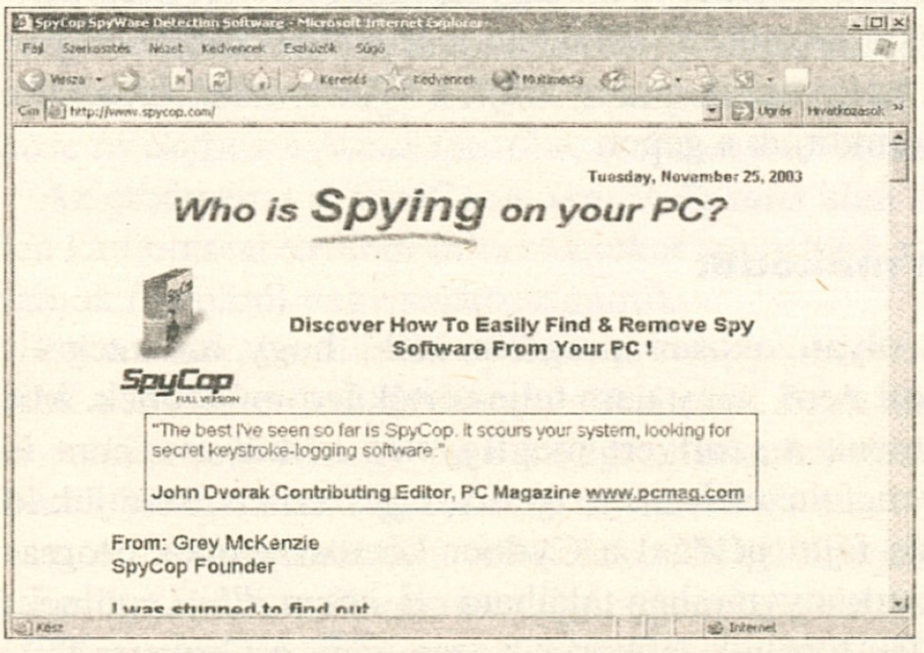
Ehhez keressünk rá egy webes keresőgépen a fájlnévre, vagy mindjárt a hozzá tartozó zippelt *cd_client.zip* változatra, töltsük le a fájlt, és csomagoljuk ki.

Ezután távolítsuk el az *Ad-aware*-rel vagy *SpyBottal* (ld. később) a Cydoor-komponenst, és cseréljük le az eredetit a kicsomagolt *cd_client.dll* dummy-fájlra. Windows 98-nál és ME-nél a *c:/Windows/System*, Windows XP-nél pedig a *c:/Windows/System32* alatt találjuk.

Ezután indítsuk újra a gépet, és használjuk a cserebörzét a szokott módon – természetesen távfelügyelet nélkül. Mert az új „dll"-fájl eljátssza a szoftvernek, hogy a Cydoor továbbra is telepítve van, valójában azonban már nem küld adatokat kifelé.

4.4 Extraprogramok egyedi esetekben

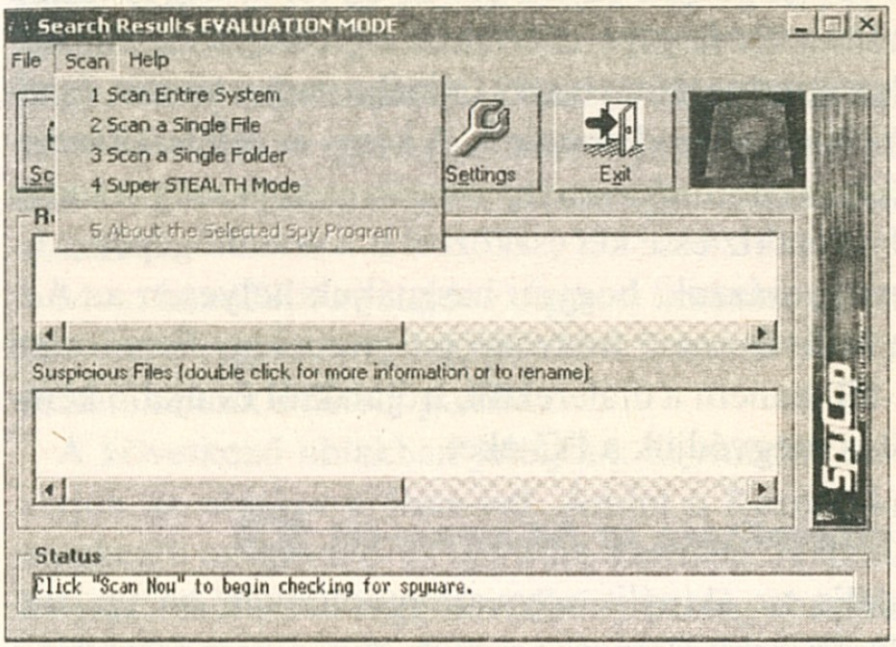
Ha nem tudjuk, melyik fájlt kell lecserélni, használjunk egy okos kis segédprogramot, amilyen például a *SpyCop*. A SpyCop különösen a keyloggerektől és a trójaiaktól véd. A program 70 dollárba kerül, és hogy kipróbáljuk, korlátozott tesztverzióban letölthető a **www.spycop.com** címről, illetve CD-mellékletünkön is megtalálható.



Tíz perc alatt megvédhetjük komputerünket – ígérik a SpyCop weboldalán

Töltsük le a próbaverziót, és telepítés után indítsuk el duplán kattintva az asztalon elhelyezett ikonjára. Ezután kattintsunk először a *Settings* gombra, és a C: mellett írjuk be a többi merevlemez-partíciót is, vesszőkkel elválasztva.

Okézzuk le, és indítsuk el az ellenőrzést a *Scan now* gombbal. Eltart néhány percig, amíg a program átkutatja a teljes merevlemezt, és előáll az eredménnyel.



Eldönthetjük, hogy az egész rendszerünket átviszgáljuk, vagy csupán bizonyos fájlokat

Ha talált valamit, azt jelöljük ki a *Suspicious Files* alatt, és kattintsunk a *Spy Info/Rename/Igen*-re. Így az érintett összetevőt a program átnevezi egy *spy* végződésű fájllá, így a továbbiakban nem fogja tudni elvégezni a kémfunkcióját. Ezután indítsuk újra a gépet.

4.5 Felhasználóbarát viselkedés

Bizonyos programokhoz olyan kis segédprogramok is léteznek, amelyek kikapcsolják a szimat-komponenseket. Ezeket úgy találjuk meg, ha egy keresőgépnek megadjuk a programneveket, valamint a „dummy" és az „adware" fogalmat. Egy példa: a GetRight letöltésvezérlő gyártója a weboldalán kifejezetten utal egy programra (**www.xright.com**) a reklám-

elemek eltávolításához, a szoftver működésének korlátozása nélkül. Természetesen a programjukba spyware-összetevőket integráló gyártók közül a legkevesebben kínálnak fel ilyen felhasználóbarát szolgáltatást. Ilyenkor azonban gyakran segítenek egy harmadik fél programjai.

4.6 Védekezés a spyware-ek ellen

Mára már olyan mennyiségű programban rejtőzik spyware, hogy óriási a valószínűsége, hogy az Ön számítógépe is érintett: a GetRight downloadmanagertől számos ZIP programig. Nem hiszi? Csinálja meg a tesztet, és távolítsa el a kémprogramokat a merevlemezéről. A kém- és reklámösszetevők hatalmas száma miatt nem minden antispy-szoftver talál meg minden bejegyzést. Ezért inkább ellenőriztesse két eszközzel is a számítógépét.

A következőkben elmagyarázzuk, hogyan használjuk helyesen az *Ad-aware* és *Spybot Search & Destroy* freeware programokat. Ezzel nem csak az ad- és spyware-től, hanem a dialerektől, trójaiaktól és újabb kémprogramok telepítésétől is megvédjük a PC-nket.

4.6.1 Spyware-ek eltávolítása az Ad-aware-rel

Az *Ad-aware* megtalálja az aktuális spyware-modulokat, ha update-funkciójával mindig a legfrissebb állapoton tartjuk. A program átkutatja a memóriát, a Windows Registry-t, valamint azokat a merevlemezeket és meghajtókat, amelyeket előzőleg rögzítettünk. Ha az Ad-aware kémprogramokat talál, azokat rögtön törölhetjük is. Töltsük le a programot a **http://lavasoft.element5.com/support/download** címről (illetve CD-mellékletünkről). Ehhez válasszuk a weboldal alján az *Ad-aware 6 Standard Editionnél* valamelyik felsorolt szervert, és a megjelenő oldalról indítsuk el a letöltést. Az alapvetően angol nyelvű programot más nyelvű (német, orosz, francia stb.) menükkel láthatjuk el, ha a Lavasoft weboldalra visszatérve, a *Languagepack*-ra kattintunk.

A telepítéshez kattintsunk duplán az *aaw6.exe* programfájlra, vegyünk át minden előzetes beállítást és zárjuk le *Finish*-sel a setupot. Kattintsunk duplán a *Languagepack-re*, és folytassuk a telepítést háromszor a *Next*-re kattintva.. A negyedik lépésben a kívánt nyelven kívül minden mást kapcsoljunk ki, és kattintsunk a *Next/Next/Finish* gombokra.

Az Ad-aware telepítése automatikusan létrehoz egy ikont az asztalon, amelyről elindíthatjuk a szoftvert. Ha át akarjuk állítani a programnyelvet, jobbra az Ad-aware 6.0 felirat mellett kattintsunk a *Settings* ikonra. A *Language File* mezőben válthatunk nyelvet, és a *Proceed* gombbal folytathatjuk a folyamatot.

Töltsük le az internetről az aktuális listát azokkal a spyware-szoftverekkel, amelyeket az Ad-aware-nek fel kell ismernie. Ehhez menjünk fel a webre, és az Ad-aware-ben nyomjuk le a *Check for updates now* és a *Connect* gombot. Mikor rövid idő múlva megjelenik az üzenet, hogy van új referenciafájl, válaszoljunk a letöltésre és a telepítésre vonatkozó kérdésekre igennel. Amint a program az online aktualizálás ablakban 100%-ot jelez, térjünk vissza egy kattintással a *Finish* gombra a főablakba.

Most kezdődik a tulajdonképpeni keresés: váltsunk a feladatoszlopon a *Scan now* regiszterre. Jelöljük ki a *Select drivers\folders to scan* feliratot, és kattintsunk a *Select* gombra.

A következő ablakban jelöljünk ki minden merevlemez-meghajtót és zárjuk az ablakot a *Save*-vel. Amint a *Next*-re kattintunk, az Ad-aware megkezdi az adware- és spyware-keresést. A rendszerellenőrzés a merevlemezek méretétől függően néhány percig eltarthat.

Ha az Ad-aware kémprogramot talál, kigyullad egy jel.

Egy kattintás a *Next*-re, és megnyílik egy új ablak, amelyben minden spyware-összetevőt kijelölhetünk törlésre.

Fontos! Használjuk a *Save* gombot, mielőtt a *Next*-tel eltávolítanánk a kiválasztott összetevőket a rendszerből. Ezzel készítünk egy biztonsági mentést a talált elemekről. Ezt szükség esetén az integrált Backup Managerrel visszállíttathatjuk. Ez akkor szükséges, ha egy szoftver az elemek valamelyike nélkül, amelyet az Ad-aware-rel töröltünk, egyáltalán nem, vagy csak korlátozottan működik. Ha az illető képességről, illetve programról nem akarunk lemondani, telepítsük vissza a spyware-t az említett Backup Managerrel.

Kattintsunk még egyszer a *Next*-re, és hagyjuk jóvá OK-val, hogy az Ad-aware minden kémprogramot töröljön.

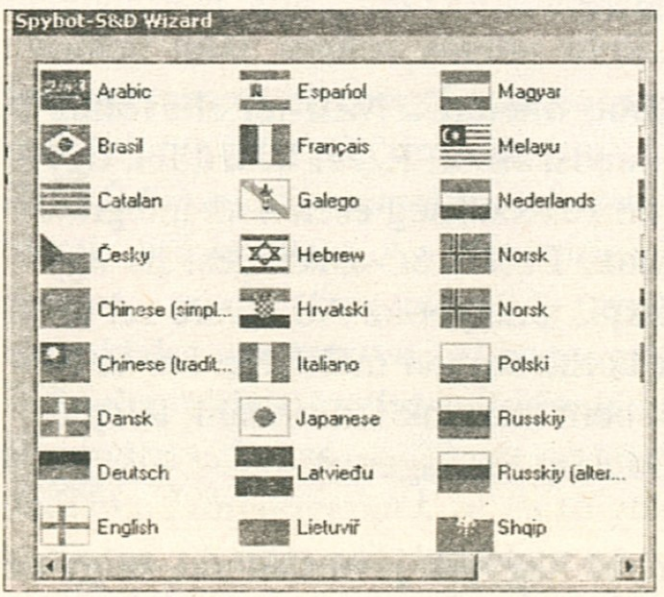
25 euróért megkapjuk az *Ad-Watch* kiegészítő programot is (**http://lavasoft.element5.com/purchase/home**). Ez a program a háttérben figyeli, hogy települ-e a rendszerre új spyware-szoftver, és ha igen, riadót fúj. Ettől kezdve tehát nem kell saját kezűleg rendszeresen ellenőriznünk a számítógépünket.

4.6.2 Átfogó védelem a SpyBot Search & Destroy-jal

Jó kiegészítést jelent az Ad-aware-hez a *SpyBot Search & Destroy*. Ez az ingyenes program ugyanis nemcsak adware-t és spyware-t keres, hanem a betárcsázókat, keyloggereket és trójaiakat is felderíti és eltávolítja. Ehhez járul még, hogy blokkolja a veszélyes ActiveX-vezérlőket, valamint a cookie-kat, és törli a böngészőből a felkeresett weboldalakat.

Mentsük a szoftvert a PC-nkre, a **http://security.kolla.de/** oldalon a *spybots12.exe* fájlra kattintva, ahol az 1.2 a verzióra utal (a program CD-mellékletünkön is megtalálható.). A mentett fájlra duplán kattintva telepítsük a programot, és hagyjunk jóvá minden setup-lépést *Next*-tel (és persze ne feledjük jóváhagyni a licencfeltételeket sem).

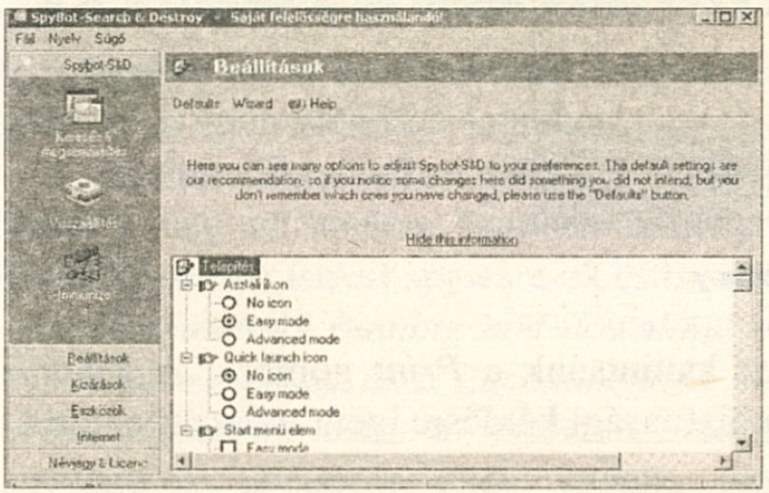
A programot ne az asztalon található ikonról indítsuk, hanem a *Start/ Minden program/ Spybot Seaarch & Destroy/SpyBot-S&D (advanced mode)* útvonalon. Ez azért jobb így, mert a szoftver két verzióban – *advanced* és *easy,* azaz haladó és kezdő (könnyű) – települ fel, és a haladóbb változat több beállítási lehetőséget kínál.



A nyelvek között a magyar is szerepel

Az első programindításnál kattintsunk a *Nyelv* menü alatt a magyarra. (Ettől a programfelület egy része magyarul jelenik meg.) Egy jogi útmutató felhívja a figyelmet, hogy előfordulhat, hogy egy programot nem használhatunk tovább, ha a Spybottal eltávolítjuk belőle a reklámmodult. Kétség esetén nézzünk ennek utána a szoftver licencfeltételeiben.

Figyelmeztetés: Ha – mint példánkban – már telepítve van az Ad-aware, akkor az Ad-aware spyware-t sejt a SpyBotban, mert ez a program archívfájlokat készít az eltávolított spyware-komponensekről, és az Ad-aware pontosan ezeket találja meg. Ezek azonban ártalmatlanok, mert karanténban vannak izolálva. Tehát ne izguljunk: az Ad-aware miatti riasztást nyugodtan átugorhatjuk, sőt, ezt is kell tennünk.



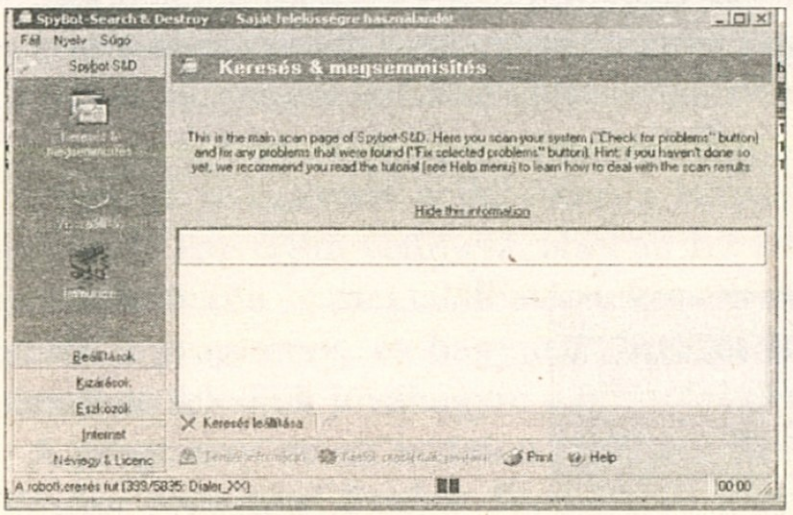
A „magyar" oldalak nyelvezete kissé vegyes

Először aktualizáljuk a SpyBot spyware-listáját. Lépjünk kapcsolatba az internettel, és kattintsunk a programban a *Keresés-re*. Jelöljünk ki minden rövid ideje megjelent frissítést, és kattintsunk a *Letöltés-re*.

Amint lezárult a frissítés, a program újraindul, és a bal ablakszélen megjeleníti a feladat-, illetve eszköztárakat. A *Beállítások* és az *Eszközök* előzetes beállításait hagyjuk meg. Ha már tudjuk, hogy egy bizonyos program vagy egy cookie spyware-összetevőit nem szeretnénk eltávolítani, kattintsunk a *Kizárások*-ra. Ez akkor célszerű, ha egy meghatározott betárcsázót használunk, vagy egy bizonyos weboldal elérését cookie-val

szeretnénk kényelmesen megvalósítani. Az *All Product,* iletve *Cookies* regiszterlapokon kapcsoljuk be a speciális kivételünket.

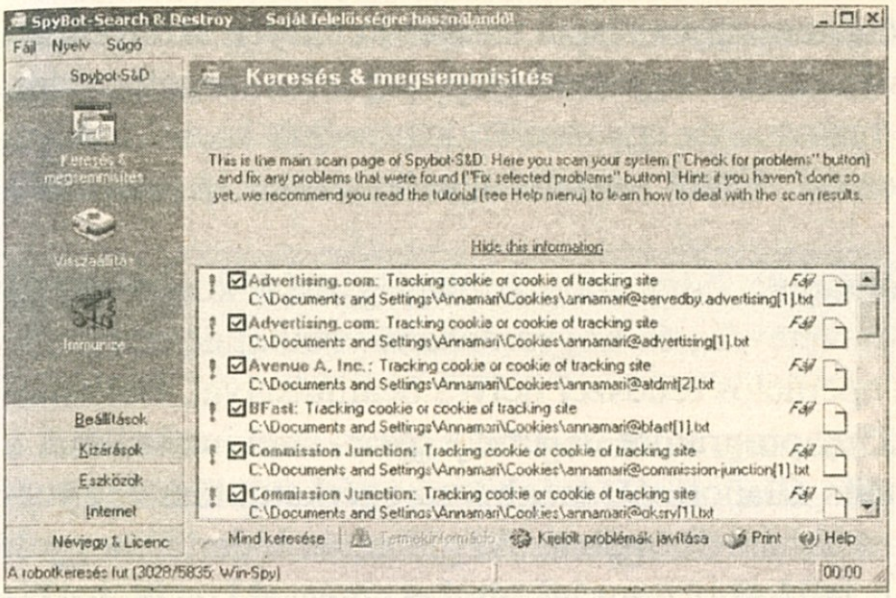
A rendszerünk ellenőrzéséhez kattintsunk fent a *Keresés & megsemmisítés* -re. A keresés egy percig tart. És ami még fontos: ne töröljük azonnal az öszetevőket, hanem jelöljük ki egymás után a felsorolt bejegyzéseket, és kattintsunk mindegyiknél balra lent a termék leírására. Egy kiegészítő ablak tájékoztat – angol nyelven – arról, hogy a káros elemek mit művelnek a PC-n.



Munkában a SpyBot Search & Destroy

Az eredmény megőrzéséhez kattintsunk a *Print* gombra. A *Kijelölt problémák javítása* gombról a biztonsági kérdésre igent válaszolva töröljük a leleplezett károkozókat.

Ha ezután egy program, amelyből eltávolítottuk a reklám- vagy kémmodult, nem fog rendesen működni, a Spybot az említett backuppal lehetőséget kínál ezeknek az elemeknek a visszakapcsolására. Ehhez kattintsunk a feladatlistán a *Visszaállítás*-ra. Jelöljük ki a következő listán az érintett bejegyzést, és kattintsunk a *Kijelöltek visszaállítására,* hogy a programot ismét használhatóvá tegyük.



A lista kissé ijesztő...

4.6.3 Védelem az újabb károkozók ellen

A SpyBot azt is lehetővé teszi, hogy a számítógépünket ellenállóvá tegyük az új spyware-ekkel szemben.

A védelem három síkon működik: A *Permanent IE immunity* úgy változtatja meg az Internet Explorer néhány belső beállítását, hogy ezzel blokkolja a már ismert spyware-ek és hasonló fenyegetések feltelepülését.

A *Permanently running bad download blocker for IE* blokkolja a további károkozókat, és a *Recommended miscellaneous protections* még biztonságosabbá teszi a rendszert. Hogy a számítógépünket az új spyware-ek telepítése ellen védjük, kattintsunk a feladatlistán az *Immunize*-ra és az *OK*-ra. Nyomjuk le az *Immunize* és az *Install* gombokat, és jelöljük ki egészen lent mindhárom beállítást. Végül a SpyBotra éppúgy érvényes, mint az Ad-aware-re: hozzuk a programot a *Keresés* gombbal mindig a legújabb állapotúra, mielőtt újból spyware-keresőbe küldenénk.

4.7 Hazatelefonál a Windows?

Mintha nem volna elég, hogy a PC-nket sok spyware-program nyilvánvaló módon megpróbálja kifigyelni, most még az aktuális Windows verziónk is állandóan kapcsolatot tart a gyártójával!

Hogy az operációs rendszer egyes részei valójában milyen információkat küldenek a Microsoftnak, azt a gyakorlatban alig lehet megállapítani. Ezért menjünk inkább biztosra, és egyszerűen kapcsoljuk ki a Windows XP potenciális kémelemeit. Ezzel semmit sem veszítünk a sokoldalú funkcionalitásból.

Az alábbiakban bemutatjuk, hogy milyen megfigyelési kockázatokat rejtenek az egyes XP-összetevők, és hogyan akadályozhatjuk meg a lehetséges kémkedést az operációs rendszer helyes beállításaival. Bemutatjuk a freeware *XP-AntiSpy* programot is, amely gyors áttekintést kínál a fontos beállítások aktuális állapotáról, méghozzá egérkattintással, gyorsan, egyszerűen testre szabható formában. Végül az is kiderül, hogyan zárhatjuk le az újonnan fellépő biztonsági réseket, még akkor is, ha kikapcsoltuk az automatikus frissítést.

4.7.1 Az XP-összetevők ellenőrzésének kikapcsolása

Kezdetben főleg a Windows XP termékaktiválása került gyanúba, hogy személyes adatokat vagy hardverinformációkat küld a Microsoftnak. Igazságtalanul, mint azt több szakértői vélemény is megállapította. Ezek szerint a Windows XP-nek és az Office XP-nek, valamint ezek egyes alkalmazásainak, mint amilyen például a Word 2002, a kényszeraktiválása, amelyet meg kell különböztetnünk az önkéntes regisztrálástól, névtelenül történik és megbízható.

Az operációs rendszer telepítése után különösen a következő kilenc segédprogram gyanús, hogy információkat közvetít a Microsoft felé a PC-ről, illetve tulajdonosáról.

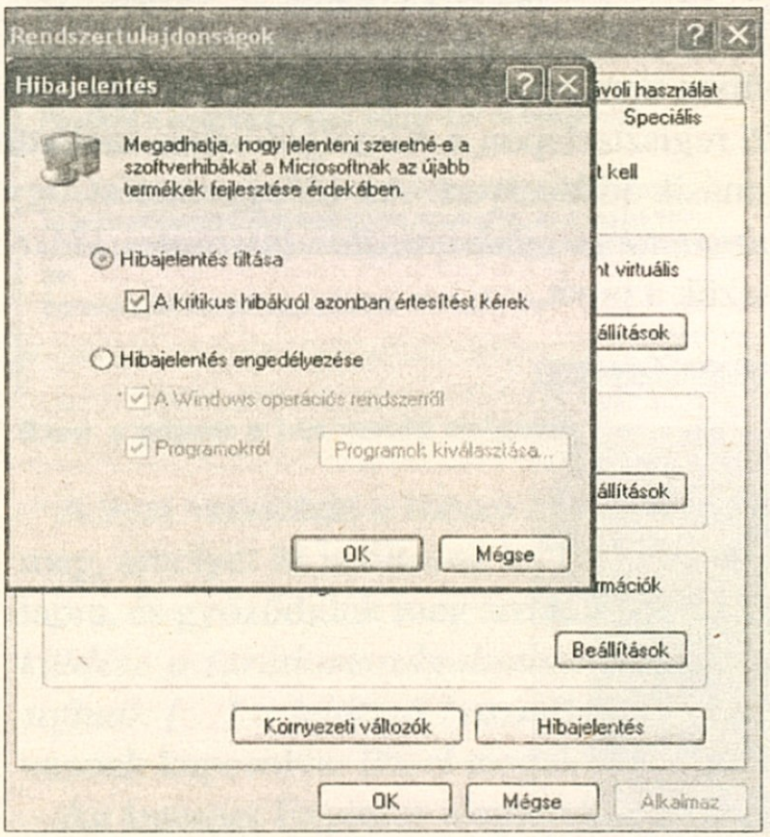
Az úgynevezett *WindowsUpdate* az aktuális frissítésekkel és bővítésekkel mindig a legújabb állapoton tartja a számítógépünket. Ami elsőre kényelmesen hangzik, mert nem kell többé frissítéseket keresgélnünk, az a kémkedés veszélyét hordozza. Hiszen az XP felismeri, hogy online kapcsolatban vagyunk-e és hogy mikor, és felhasználja az internetkapcsolatot, hogy letöltéseket keressen az update-oldalon. Eközben a Microsoft-szerver egészen pontosan látja, milyen összetevők vannak telepítve a számítógépünkre.

A három beállítási lehetőség mellett, amelyekkel többé-kevésbé automatikusan futtathatjuk a frissítést, az operációs rendszer arra is kínál le-

hetőséget, hogy ezt a funkciót teljesen kikapcsoljuk. Kattintsunk ehhez a jobb egérgombbal a *Sajátgép* ikonra az Asztalon, válasszuk a *Tulajdonságokat,* és az *Automatikus frissítések* regiszterlapon távolítsuk el a pipát *A számítógép automatikus frissítése...* elől.

Fontos. Ennek a beállításnak a módosításához rendszergazdaként kell bejelentkezve lennünk.

A Windows automatikus hibajelentése , minden alkalommal megkérdezi, hogy küldjön-e értesítést a Microsoftnak, ha egy program lefagy. Hogy eközben mi mindent közöl a gyártóval, azt ki tudja. Akit idegesít ez a felszólítás, kapcsolja le tartósan ezt az ablakot.



Letilthatjuk a hibajelentést

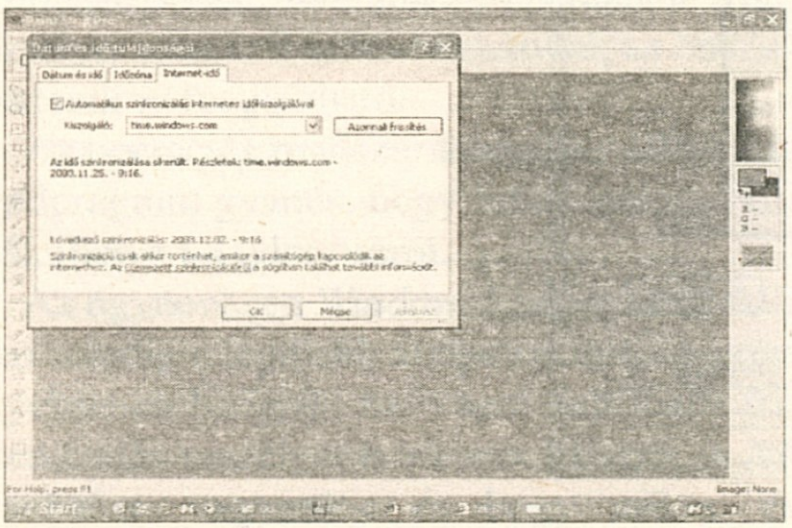
Ehhez nyissuk meg újból egy jobb egérgombkattintással a Sajátgép/ *Tulajdonságokat*, és a *Rendszertulajdonságok* ablakban a *Speciális* regiszterlapon nyomjuk le a *Hibajelentés* gombot, és kapcsoljuk be a *Hibajelentés tiltása* beállítást.

Választhatjuk a *Program kiválasztása* gombot is, hogy a *Soha ne legyen hibajelentés az alábbiakhoz* területhez adjuk hozzá a gyakran lefagyó programokat. Az itt felsorolt programok le lesznek zárva, anélkül, hogy véletlenül hibajelentést küldhetnénk róluk a Microsoftnak. Ezen a módon már eleve kizárhatjuk a küldésből a problémás alkalmazásokat.

4.7.2 A Media Player és a böngésző

Most három összetevő, az időszinkronizálás, a Media Player és az Internet Explorer következnek. Mindhárom Windows XP-be integrált modul adatokat küld a Microsoftnak.

Alapértelmezésben az időszinkronizálás kapcsolatba lép a Microsofttal, és kiegyenlíti a PC belső óráját a standard idővel. Hogy ezt megakadályozzuk, kattintsunk a *Start/Vezérlőpult/Dátum és Időre*. Ha az automatikus órabeállítás – meg kell adni, létező – előnyeit továbbra is élvezni szeretnénk, és csak a Microsoftban nem bízunk meg, válasszunk egy másik időszervert. Az *Internetidő* regiszterlapon a *Kiszolgáló lista* melletti nyílra kattintva találunk egy másik időszervert. Az időegyeztetést úgy tilthatjuk le teljesen, ha az *Automatikus szinkronizálás internetes időkiszolgálóval* beállítás elől elvesszük a pipát.



Itt választhatunk másik időszervert

A Media Player alapértelmezésben ugyancsak arra van beállítva, hogy állandóan kapcsolatba lépjen a Microsofttal, és információkat közvetítsen. Mivel a 8-as és a 9-es verzió lényegesen különbözik egymástól ab-

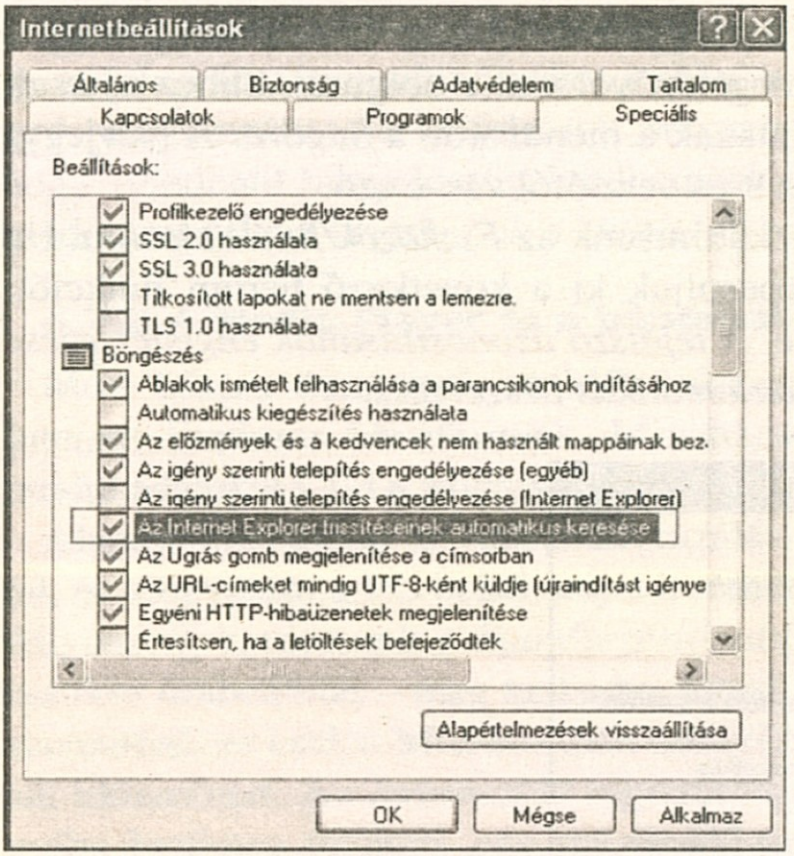
ban, hogyan kell kikapcsolni a felügyeletet, először nézzük meg, hogy a legújabb változattal, vagy a megelőzővel van-e dolgunk. Ehhez nyissuk meg a Media Playert, és kattintsunk a menüsoron a *Súgóra.* A Névjegyből látható, hogy a 8-as vagy a 9-es verziótól van-e szó.

Zárjuk be az infóablakot, és kattintsunk az *Eszközök/Beállításokra.* Ha a 8-as verziót használjuk, kapcsoljuk ki a következő három funkciót: *Kodekek automatikus letöltése, A lejátszó azonosításának engedélyezése internetoldalaknak* és *Licenc automatikus beszerzése.*

Ezen a gépen a 9-es verzió dolgozik

A 9-es verzióban a három beállítás közül először csak az elsőt találjuk meg, amelyet itt is tiltsunk le. Ezután váltsunk az *Adatvédelem* regiszterlapra, és győződjünk meg arról, hogy *A lejátszó egyedi azonosítójának elküldése a tartalomszolgáltatónak* valamint az *Elősegítem .[…]a Microsoftnak […].a lejátszó használatára vonatkozó adatokat.* beállítások ki vannak kapcsolva. Ezzel megakadályozzuk kifelé a kommunikációt.

Az Internet Explorer alapértelmezésben a teljes internetezési magatartásunkat figyeli, hogy megtalálja az úgynevezett rokonlinkeket. Eközben többek között az IP-címünket, a felkeresett oldalak teljes címét és még sok mást is elküld. Hogy a böngésző kommunikációját megakadályozzuk, először nyissuk meg az *Eszközök/Internetbeállítások* alatt a *Speciális* regiszterlapot. Itt tiltsuk le *Az Internet Explorer frissítésének automatikus ellenőrzése* funkciót (egészen a lista tetején) és az *Integrált Windows-*



Megakadályozhatjuk a böngésző kommunikációját

hitelesítés engedélyezése (alsó harmad) funkciót. Kapcsoljuk viszont be a *Passzív FTP használata* beállítást. Zárjuk be az *Alkalmaz* gombbal az ablakot, és indítsuk újra a gépet.

Az *Alexa* nevű spyware-t, amely az internetezési szokásainkat figyeli, a következőképpen tilthatjuk le: indítsuk el a Rendszerleíró adatbázis-szerkesztőt (a *Registry*-t), a *Start/Futtatásra* kattintva, a *regedit* paranccsal.

Ha elindult a *Registry,* azt a következő módosítás előtt mindenképpen mentsük. Ehhez kattintsunk a menüsoron a *Fájl/Exportálásra*, adjunk egy jelentéssel bíró nevet, és mentsük a kereken 50 Mbájtos fájlt CD-re vagy egy második merevlemezre. Közben figyeljünk arra, hogy az *Exportálási tartomány* alatt az *Összes ág* legyen megjelölve.

A mentés után nyissuk meg a *HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Extensions\c95fe080-8f5d-112d-a20b-00aa003c157a* kulcsot. Jelöljük ki ezt a mappát, nyomjuk le a **Delete** gombot, és a megerősítést kérő kérdésre válaszoljunk *Igen-nel.* Ezzel töröljük a teljes mappát és vele a spyware-t.

4.7.3 További összetevők eltávolítása az XP-ből

Miután bizonyos beállításokat már megváltoztattunk, illetve néhány összetevőt, mint amilyen az Alexa is, eltávolítottunk, töröljünk még további részeket, amelyeken keresztül a Microsoft potenciálisan információkat kaphat rólunk és a PC-nkről.

További fogást kínál a *távoli támogatás,* amely manipulálható Javascriptekből áll. Ezt a távsegítséget, amelynek a keretében a segítő a teljes ellenőrzést megkapja a számítógépünk fölött, amúgy is csak olyan személytől kérjük, akiben maradéktalanul megbízunk. A Microsoft azonban alapértelmezésben két olyan felhasználói fiókot is integrált a rendszerbe, amelyekről a számítógépünk távoli elérése lehetséges. Mivel nem világos, hogy a Microsoft ezáltal tud-e és milyen körben elérést szerezni a rendszerünkre, töröljük ezt a két fiókot. Ehhez kattintsunk a *Vezérlőpult/Felügyeleti eszközök/Számítógép-kezelés/Helyi felhasználók és csoportok/Felhasználókra.* Az általunk létrehozott fiókok, illetve a vendég-, illetve rendszergazda hozzáférés mellett megtaláljuk a *Segítségnyújtó* és a *Support_388945a0* bejegyzéseket is. Jelöljük ki e kettő közül először az egyiket, nyomjuk le a **Delete** gombot a billentyűzeten, és hagyjuk jóvá *Igen-nel* a törlést. Ismételjük meg ezt a lépést a második fiókra is.

Még ha nem is jelentkeztünk be a Windows Messengerbe, következésképp soha nem is használtuk, ez az XP-komponens akkor is rendszeresen küld adatokat a Microsoftnak. Hogy ezt megakadályozzuk, két lehetőségünk van: vagy kompletten töröljük a Messengert, vagy átnevezzük a kényes fájlokat. Az utóbbinak megvan az az előnye, hogy a folyamatot bármikor visszafordíthatjuk, ha egyszer mégis használni szeretnénk.

Az időleges kikapcsoláshoz menjünk a Windows Intézőben a *c:\windows\messenger* mappába, és jelöljük ki benne az *msmsg.exe* fájlt. Nyomjuk le az **F2** billentyűt, és írjuk át az *exe* végződést pl. *alt*-ra. Ezen a módon működésképtelenné tesszük a Windows Messengert, de ha a fájlt visszanevezzük az eredetire, akkor újból használhatóvá válik.

Ahhoz, hogy teljes mértékben eltávolítsuk ezt a kommunikációs programot, először kattintsunk a jobb egérgombbal a Tálcán jobbra lent a *Messenger* ikonra. A helyi menüből válasszuk a *Bezárás-t.* Ezután zárjunk be minden programot, kattintsunk a *Start/Futtatás*-ra, és a *Megnyitás* mezőbe írjuk be: *RunDLL32 advpack.dll, LaunchINFSection*

%windir%\INF\msmsgs.inf,BLC.Remove. Figyeljünk az üres karakterekre, valamint a kis- és nagybetűkre. Kattintsunk az OK-ra, és a biztonsági kérdésre válaszoljunk *Igen-nel*. A Windows megerősíti, hogy eltávolította a Messengert.

Egy bizonyos *RegDone*-bejegyzésen keresztül a Windows XP ugyancsak kapcsolatot vesz fel a Microsofttal, és adatokat küld. Ez addig történik, míg a *RegDone*-értéket 1-re nem állítjuk a *Registry*-ben.

Ezt az adatátvitelt megakadályozandó, mint az előzőekben leírtuk, indítsuk el a Registry-t. Nyissuk meg a *HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion* kulcsot, és kattintsunk a jobb egérgombbal a *RegDone*-ra. A helyi menüből válasszuk a *Módosítás-t,* az értékhez írjuk be: 1. Hagyjuk jóvá OK-val, és zárjuk be a szerkesztőt.

4.7.4 Automatikus frissítés nélkül is a legújabb állapoton

Ha az *Automatikus frissítések* funkciót – akár manuálisan, akár az *XP-AntiSpy*-jal – kikapcsoltuk, a jövőben magunknak kell patch-ekről és frissítésekről gondoskodnunk. Ez különösen akkor fontos, ha egy új biztonsági rést fedeznek fel, és a Microsoft ennek a bezárásához kínál patch-et.

Hogy biztosra menjünk, rendszeresen el kell olvasnunk a Microsoft biztonsági hirdetményét **(http://www.microsoft.com/hun/technet/default.mspx).** Azt is kérhetjük, hogy a közleményeket küldjék el nekünk mailben, ha a **http://register.microsoft.com/regsys/pic.asp** weboldalon megadjuk a mail-címünket, és a *Continue*-val jóváhagyjuk.

Ennél az eljárásnál azonban minden alkalommal el kell döntenünk, hogy fontos-e az adott figyelmeztetés számunkra. Ha fontosnak tűnik, görgessük le addig a weboldalt, amíg megtaláljuk a *Letöltési cím ehhez a patch*-hez feliratot. Ha több hely is rendelkezésre áll, nézzük meg pontosan, melyik a számunkra igazi. Kövessük a letöltés linket, és az azt követő, specifikus telepítési utasításokat.

Ne használjuk az automatikus *WindowsUpdate*-et *(Start/Minden program/WindowsUpdate)*. Mert ennél egy Microsoft-szerver ellenőrzi a rendszerünket, és eközben lehet, hogy adatokat is küld, tehát éppen azt teszi, amit nem akarunk.

Végül is az a fontos, hogy egy átfogó patch vagy update telepítése után minden elvégzett beállítást még egyszer ellenőrizzünk, mert közben bizo-

nyos értékek visszaállítódnak az alapértelmezésekre. Csak így lehetünk biztosak benne, hogy kikerüljük a Microsoft megfigyelését.

Ha le szeretnénk mondani az értesítéseket az új update-ekről és patch-ekről, kattintsunk ismét a **http://register.microsoft.com/regsys/** címre, és írjuk be a mail-címünket. Ezután hamarosan kapunk egy új e-mailt a *Microsoft Security Notification Service*-től, amelyre a tárgysorban az *Unsubscribe* szóval kell válaszolnunk.

4.7.5 A fölösleges szolgáltatások kikapcsolása

Az XP operációs rendszer egy sor úgynevezett szolgáltatást is kínál, amelyek rendszerindításkor automatikusan elindulnak. Ezek részben fontosak a biztonsághoz, ám minden esetben fékezik a rendszert. Általánosan érvényes, hogy nem minden Windows XP-számítógépen vannak ugyanazok a szolgáltatások, mert ezek a telepített hálózati összetevőktől, meghajtóktól és alkalmazásoktól függnek.

Mielőtt módosítanánk a szolgáltatásokat, feltétlenül mentsük el a Registry megfelelő ágát. Indítsuk el újból a Registry-szerkesztőt, nyissuk meg a *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services* kulcsot, és kattintsunk jobb egérgombbal erre a mappára. A helyi menüből válasszuk az *Exportálást,* adjunk meg egy fájlnevet, és mentsük a reg-fájlt. Ha később problémák adódnak, dupla kattintással erre a fájlra ismét hozzáadhatjuk a Registry-hez a teljes ágat.

A számítógépünkön aktuálisan rendelkezésre álló szolgáltatások listáját úgy nyitjuk meg, hogy a *Start/Futtatásra* kattintunk, majd beírjuk a *services.msc* parancsot. A Windows minden szolgáltatásról egy kis leírást, beállításokat és állapotjelentést mutat. Fontos az automatikus indítás három beállítási lehetősége: *Automatikus, Kézi* és *Tiltás,* amelyek az *Indítási típus* oszlopban vannak.

Egy szolgáltatás indítási típusának átállításához kattintsunk duplán az illető sorra. Először ellenőrizzük a *Függőségek* regiszterlapon, milyen további rendszerösszetevőkre van szüksége az adott szolgáltatásnak a hibátlan működéshez. Ez alatt azt is látjuk az ablakban, hogy milyen további szolgáltatások függenek az aktuálisan kijelölttől.

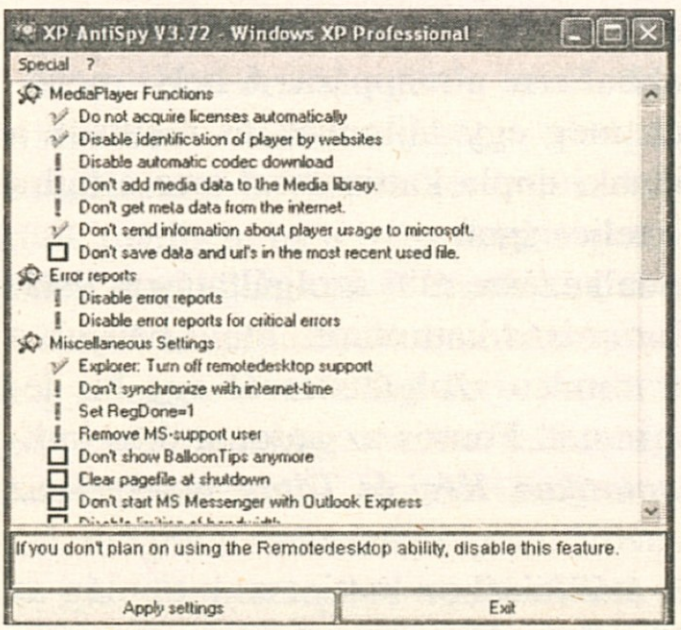
Csak olyan szolgáltatásnál változtassuk az *Általános* regiszterlapon az indítás típusát kézire vagy tiltásra, amely *A következő rendszerösszetevők*

ettől a szolgáltatástól függnek ablakban a *Nincs függőség* bejegyzést mutatja. A Microsoft-megfigyelés szempontjából különösen az *Automatikus frissítések* és a *Hibajelentési szolgáltatás* fontosak: ezeknél állítsuk be a tiltást.

Ha további szolgáltatásokat is ki akarunk kapcsolni, mindig csak egy beállítást változtassunk meg egyszerre, és utána ellenőrizzük a PC működését.

4.7.6 Kényelmesen az XP-AntiSpy-jal

Most már tudjuk, milyen beállításokat kell az XP-ben megváltoztatni ahhoz, hogy minimálisra csökkentsük a Microsoft általi ellenőrzés kockázatát. Ugyanerről az eredményről gondoskodik a CD-mellékletünkön is megtalálható freeware *XP-AntiSpy* program is – csak sokkal kényelmesebben. Az XP-AntiSpy mind az eredeti Windows XP-hez, mind a szervizcsomag (Service Pack) 1-hez alkalmas: és ez egyaránt érvényes a *Home* és a *Professional* verzióra.



Az XP-AntiSpy magyarázatot fűz minden bejegyzéshez

A biztonság kedvéért minden eddig leírt beállítást ellenőrizzünk még egyszer, miután az XP-AntiSpy-t telepítettük és futtattuk. Mert a Microsoft elméletileg minden frissítéssel beállíthatja úgy az operációs rendszert, hogy az XP-AntiSpy üresbe fusson.

Töltsük le az XP-AntiSpy legújabb verzióját a **www.xp-antispy.org** weboldalról vagy lemezmellékletünkről. Indítsuk el dupla kattintással a telepítést a mentett fájlra, és kattintsunk a *Tovább* és a *Telepítés* gombokra. A program ezután a *Minden program/ XP-AntiSpy* bejegyzés alatt jelenik meg.

A program első megnyitásakor az egyes bejegyzések rendje egy kicsit átláthatatlannak tűnik. A program azonban minden funkcióhoz kiír az ablak alján egy rövid magyarázatot, amint átvisszük az egérmutatót az illető funkció felett.

Rendszerállapottól és az előzetes beállításoktól függően maximum négy különböző ikont láthatunk.

A zöld pipa (egészen fent balra a képen) akkor jelenik meg, ha az illető funkciókat már kikapcsoltuk. A piros felkiáltójel figyelmeztetésre szolgál: ezt a beállítást meg kell változtatni! Az egyirányú utca jellel ellátott beállítások inaktívak, és csak a *Profi* beállításokban *(Speciális/Professional Setup)* aktiválhatók. A fekete dobozkák az alapjában véve nem túlzottan fontos funkció előtt állnak, amelyeknek a beállítása nem olyan lényeges.

Hogy az XP-AntiSpy el tudja végezni a rendszerben szükséges beállításokat, kattintsunk kétszer a felső, *Licencek megszerzése ne legyen automatikus* bejegyzésre. Az első kattintásnál a felkiáltójel fekete dobozkává változik, a másodikra bekapcsoljuk a funkciót. Erre a két nagy gomb közül a *Beállítások alkalmazása* alatt a bal oldali aktívvá válik. Nyomjuk le, hogy biztonságba helyezzük a számítógépünket kémkedés ellen. Csak egy pillanatig tart, míg minden fontos funkció zöld pipát kap.

Még két érdekes kiegészítő funkció van: a menülistán a *Speciális* bejegyzést, majd a *Minden beállítás visszaállítását* használva a szoftver minden megváltoztatott értéket visszaállít a Windows alapértékeire. Ezt a globális reset-et azonban ne használjuk.

Fontosabb számunkra a funkciókra szabott visszaállítás, amelyet úgy érünk el, ha a jobb egérgombbal az érintett bejegyzésre kattintunk. A megnyíló helyi menüből válasszuk ki az egyes bejegyzést, és várjunk egy pillanatot, amíg az ismét bekapcsolódik. Ezen a módon időlegesen visszakapcsolhatunk egyes funkciókat.

5 A tűzfalakról

Még ha azt is gondoljuk, hogy senki se bajlódna otthoni számítógépünk megtámadásával, ne feledjük: amint a komputerünk az internetre kapcsolódik, máris hackerek, rosszakaratú programocskák és más lopakodó veszélyek célpontjává válik. A számítógépet és a személyes adatokat megvédő saját tűzfal értékes segítség az internetről érkező fenyegetések ellen.

5.1 Tűzfal alapismeretek

5.1.1 Mire képes egy tűzfal?

A tűzfalaknak ugyanaz a szerepük, mint névrokonaiknak a házakban. Védelmi vonalat képeznek az információkat megosztó számítógépek között. A saját tűzfal rendeltetése a számítógép és az éppen használt webszerver közötti kétirányú információáramlás ellenőrzése. A tűzfal az összes, a számítógép és az internet között zajló forgalmat ellenőrzi, hogy vajon megfelel-e az bizonyos feltételeknek. Ha megfelel, átengedi azt, ha nem, megállítja. A behatolás ellen védő tűzfal megakadályozza, hogy az adatvesztéshez vagy a fájlsérüléshez vezető ártalmas betörések „megpörköljék" a gépünket.

A tűzfal mindazokat az eszközöket felkínálja, amelyek a nyilvános hálózathoz kapcsolódás alatt megvédik a magánjellegű információkat.

Kiválaszthatjuk, hogy melyek a védendő információk, például a bankkártyaszámok vagy a jelszavak. Ha nem védett helyre akarjuk elküldeni a kártyaszámot – tehát olyan helyre, ahol nem áll rendelkezésre megfelelő titkosítás – a tűzfal vészjelet ad.

A tűzfalak azt is képesek megakadályozni, hogy a webszerverek a böngészésünk közepette más kényes adatokhoz, például a címünkhöz hozzáférjenek.

A sütik (cookie-k, azaz azok a szövegfájlocskák, amelyeket egyes webszerverek helyeznek el a gépünkön) akár hasznosak is lehetnek, ha arra használják őket, hogy az ismételten meglátogatott helyek tudjanak

arról, amikor újra felkeressük őket. Így nem kell újra meg újra bejelentkeznünk, és a „bevásárlókocsink" tartalma is aktuális marad. Ebben az esetben azonban a személyi jogokkal kapcsolatos aggodalom is felmerül, nevezetesen, hogy a webböngészésünk szándékunk és tudomásunk nélküli kikémlelésére is alkalmasak.

A Java kisalkalmazásokat és az ActiveX vezérléseket is kitilthatjuk (ld. korábban), hiszen ezek is veszélyeztethetik a személyes információinkat és számítógépünk biztonságát.

Az információ felügyelete mellett a behatolás észlelésén keresztül a tűzfalak arról is értesítenek, ha valaki megpróbál ezekhez az információkhoz hozzáférni. A jelzés mellett a behatolás-érzékelés az adatok elemzése révén a védelmi rendszer gyenge pontjaira is felhívja a figyelmet.

5.1.2 Kell-e nekem a tűzfal?

Aki bármi módon, telefonvonali behívással vagy folyamatos internetkapcsolaton keresztül a webet használja, hasznát látja a saját tűzfalnak. Sok PC-használó bízik abban, hogy senki se veszi a fáradságot arra, hogy betörjön a névtelen otthoni gépére. Sajnos, ez nem igaz. Az internethez kapcsolódó összes számítógépnek van egy saját IP-címe, ami egy, az azonosítást szolgáló, egyedi számsor. A hackerek gyakran arra programozzák be a számítógépüket, hogy az véletlenszerűen kiválasztott IP-címeket vizsgáljon meg, és támadjon meg minden sebezhetőnek bizonyult gépet. A megtámadáshoz nincsen szükségük arra, hogy ismerjék a gépünket. Egy ilyen támadás sok fájl és program elvesztésébe kerülhet, főleg, ha az operációs rendszer váratlan újratelepítésére kényszerülünk emiatt.

5.1.3 Nem mindenhatók

Jó tudnunk, hogy bár a tűzfalak nyújtanak némi védelmet a férgekkel szemben, ám nem helyettesíthetik a víruskeresőt. Az aktualizált vírusölő továbbra is a biztonsági készlet alapeleme a PC-n. A tűzfal ezt csak kiegészíteni képes, hogy az internet alkalmazója a saját PC-jén lévő alkalmazásokat, illetve az ott zajló adatforgalmat ellenőrizni tudja. A tűzfal hatékonysága jelentős mértékben függ a saját viselkedésünktől, vagyis a felhasználó józan eszétől. A továbbiakban konkrétan is megvizsgálunk néhány tűzfalat.

5.2 Firewall Pro

Gyártó: bhv
Termék: Firewall Pro
Internet: www.bhv.de
Ár: 39,99 euró
Rendszerigénye: Windows 98/ME/2000(SP1)/NT4.0(SP6) XP, Pentium 133, 32 Mbájt RAM a minimum

Plusz:

- jó védelem kikerülés ellen
- kényelmes naplófájlok

Mínusz:

- nincsenek kidolgozott szabályai
- nincs setup-varázslója

A *Firewall Pro* szabálykészítő varázslója apró részletekkel is szolgál, de ezek csak a haladókon segítenek. Ezen kívül minden engedélyezett alkalmazás komplett szerverjogok birtokába jut, amit utólag a haladó beállítások között kell megváltoztatni. A program sajnos nem rendelkezik a kezdőknek való, előre gyártott szűrési szabályokkal. Viszont a haladók számos szűrési szabályhoz való konfigurálási lehetőségre, illetve egy kiváló log-funkcióra is bukkanhatnak. Ez megengedi a kapcsolatok adott jellemzők, mint például az idő, a protokoll, az IP-cím vagy port szerinti rendezését is. Tesztünk során a Firewall Pro a porttól függetlenül felismert egy veszélyes NetBusPro-szervert és nem engedte magát erőszakkal bezárni.

Összegzés: Aki először használ tűzfalat, az jobb, ha kerüli a Firewall Pro-t. A haladó számára viszont kiváló biztonsági megoldás.

5.3 Norman Personal Firewall 1.4

Gyártó: Norman
Termék: Norman Personal Firewall 1.4
Internet: www.norman.de
Ár: 39 euró
Rendszerigénye: Windows 95/98/ME/2000/NT/XP, Pentium, 64 Mbájt RAM a minimum

Plusz:

- számos szűrő
- Freshie's varázsló

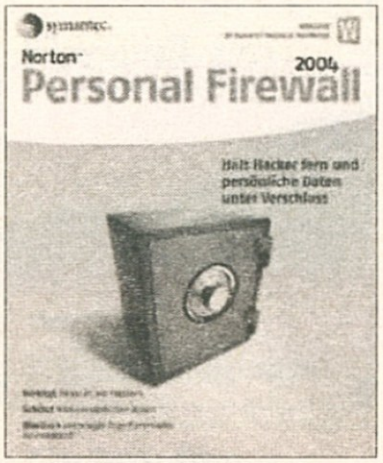
Mínusz:

- portfelügyelet
- spártai szabálykezelő

A *Norman Personal Firewall* Freshie's varázslója segít a konfigurálásban, ám túl nagy segítséget azért ne várjunk tőle. Alig tartalmaz olyan tippeket, amelyek segítenek a laikusnak a döntéshozatalban. A haladónak viszont a szabályszerkesztő nem fog gondot okozni. A tűzfal naplózó funkciója kényelmesebb is lehetne. Sajnos a tűzfal a megfelelő beállítás ellenére is válaszolt egy ping-kísérletre, így a támadó számára láthatóvá vált. A program azt sem jelezte, ha egy szerverport megnyílt. A kikerülési kísérleteknél azonban csak a *Firehole* tudta átverni a Normant. A program egy MobileCodes szűrő, reklámtiltó és PopUp-blokkoló mellett webtartalom-szűrővel is rendelkezik.

Összegzés: A haladó megbarátkozhat ezzel a programmal, ha kibékül a portkezelés hiányosságaival és a spártai naplózó funkciókkal.

5.4 Norton Personal Firewall 2004



Gyártó: Symantec
Termék: Norton Personal Firewall 2004
Internet: www.symantec.com
Ár: 49,95 euró
Rendszerigénye: Windows 98/ME/2000//XP, Pentium 133, 32 Mbájt RAM a minimum

Plusz:

- szabályszerkesztő, varázslók
- portkezelés

Mínusz:

- manipulált programok kezelése
- nincs szabályexport lehetőség

A *Norton Personal Firewall* a 2004-es verzióban is számos felhasználóbarát varázslóval támogatja a felhasználót. A nyitott portokat bezárja, és letiltja a támadási kísérleteket. A kényelmes szabályszerkesztő automatikusan felismeri a fontosabb internetes alkalmazásokat, és nem zavarja érthetetlen kérdésekkel a laikusokat. A haladó tetszőlegesen tovább bővítheti a szabályokat. Sajnos a beállítások nem exportálhatók, viszont a program az összes kikerülési kísérletet felismerte. A szabályszerkesztő azonban a manipulált programokat új alkalmazásként jelzi, ahelyett, hogy a manipulációra figyelmeztetne.

Összegzés: A Norton Personal Firewall 2004 a kezdőket támogatja, és a haladóknak is számos beállítást kínál.

5.5 PC Firewall 2004

Gyártó: Buhl
Termék: PC Firewall 2004
Internet: www.buhl.de
Ár: 49,95 euró
Rendszerigénye: Windows 98/ME/2000//XP, Pentium 233, 32 Mbájt RAM a minimum

Plusz:

- szabályszerkesztő, szabályvarázsló
- áttekinthető felület

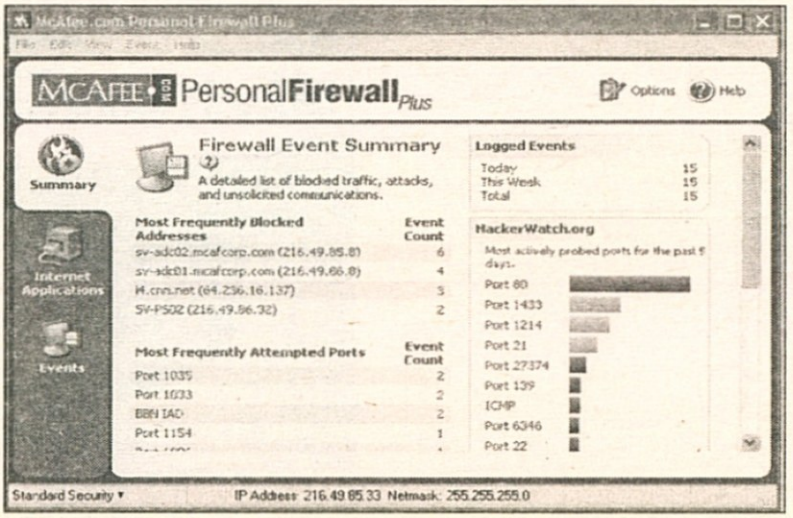
Mínusz:

- nincs kikapcsolás elleni védelme
- nem figyelmeztet a nyitott portra

A *PC Firewall* egy kiváló varázslót kínál, amelyik a legtöbb alkalmazáshoz előre gyártott szabályzatrendszert javasol, s a felhasználónak csupán nyugtáznia kell. A program rendezett felület mögött húzódik meg. A profik érdekes szabályszerkesztőt és kényelmes naplómegjelenítőt is találnak. A programot sajnos a jelszavas védelem ellenére is erőszakkal be lehet csukni, és a nyitott szerverportokra sem figyelmeztet, még ha az alkalmazások a *Nyitott portok* rovatban meg is jelennek. A program számos szűrőt is tartalmaz a *Plug-In*-ek alatt.

Összegzés: A portkezelés gyengéitől eltekintve a program mindenekelőtt a szabálykezelésével, naplófunkciójával és a dobozban található kiegészítésekkel tündöklik, így kezdőknek és haladóknak is melegen ajánlható.

5.6 Personal Firewall Plus



Gyártó: McAfee
Termék: Personal Firewall Plus
Internet: www.mcafee.com
Ár: 44,95 euró
Rendszerigénye: Windows 2000 Pro/XP/ME/98, Pentium 133, 32 Mbájt RAM a minimum

Plusz:

- felhasználó-támogatás, felület
- dokumentáció, súgó

Mínusz:

- korlátozott szabályrendszer
- 2 kikerülési teszten is megbukott

A McAfee-féle *Personal Firewall Plus* kompletten átdolgozott, áttekinthető felületet kínál, s a biztonsággal kapcsolatos eseményeket az *Összefoglalás* rovatban áttekinthetően jelzi. Az alkalmazások letilthatók, kimenetre vagy teljes mértékben is engedélyezhetők. A Personal Firewall Plus a haladók számára, a rendszerszolgáltatások kivételével, semmilyen játékteret nem kínál a finomabb szabálybeállításhoz. A program a hiányzó komponenskezelés miatt két kikerülési teszten is megbukott.

Összegzés: A haladók a korlátozott szabályrendszer miatt kerüljék a Personal Firewall Plus-t. A kezdőknek a felügyeleti gyengéktől eltekintve jól áttekinthető, rendezett felületű eszköznek bizonyulhat.

5.7 ZoneAlarm Pro 4

Gyártó: S.A.D.
Termék: ZoneAlarm pro 4
Internet: www.s-a-d.de
Ár: 49,99 euró
Rendszerigénye: Windows XP/2000 Pro/98SE/ ME, Pentium 233, 64 Mbájt RAM a minimum

Plusz:

- „kikerülhetetlen", mail-szűrő
- hatékony szabályszerkesztő

Mínusz:

- kissé nehézkes szabálykészítés

A *ZoneAlarm Pro 4* egy setup varázslóval és egy rövid tutoriallal indul. Az online súgó és a szabályrendszeri varázslóban lévő *Alert Divisor* segítségével a kezdő értékes tippeket kap. A program valamennyi átverési kísérletet sikerrel kivédett, és nem hagyta magát erőszakkal bezárni sem. Átfogó, a magánszférával kapcsolatos beállítási lehetőségekkel rendelkezik, így például letiltja a reklámokat, a JavaScript-et, vagy az ActiveX-et és kiüríti az Internet-cache-t. A *Mailsafe* funkció a potenciálisan veszélyes levélmellékletektől véd, és megtiltja a férgek általi tömeges levélkiküldést. A program használata során meg kell barátkoznunk a kissé nehézkes szabálygenerálási eljárásokkal.

Összegzés: A ZoneAlarm Pro 4 biztonságtechnikai szempontból a tesztmezőny élén áll. Széles funkcióterjedelmének és súgó opcióinak köszönhetően kezdők és haladók számára egyaránt érdekes.

6 Teljes biztonságban

Vírusok, trójaiak, spyware-ek, betárcsázók, spam-ek – amint azt már eddig is láttuk, az interneten csak úgy hemzsegnek a gonosztevők. Reméljük, hogy mire e fejezet végére érnek, valóban teljes biztonságban lesz a számítógépük.

6.1 Internetes IQ-teszt: A hét legfontosabb tévhit

Sokan böngésznek közülünk az interneten, vannak, akik vásárolnak, netán bankolnak is, s teszik mindezt annak a halvány tudta nélkül, hogy ha egyszer mi ki tudunk lépni a világba az otthoni gépünkről, akkor a világ is be tudja tenni bakancsát a gépünkre. Ellenőrizzük le, mit tudunk a számítógépes kockázatokról, és lehet, hogy meg fogunk lepődni néhány elterjedt téveszmétől.

6.1.1 Az első tévhit: Van víruselhárító a gépemen, más nem kell nekem

Ez a legelterjedtebb internetes tévhit. Az igaz, hogy a víruselhárítás fontos és szükséges. De a szoftver megléte önmagában nem elegendő. Folyamatosan bukkannak fel új vírusok, tehát a vírusazonosítókat rendszeresen frissíteni kell. Még jobb, ha olyan szoftvert használunk, amely önműködően elvégzi ezt.

Ha fellépünk a netre, a víruselhárítók a védekezésnek csak egy részét végzik el (megakadályozzák a vírusokat abban, hogy megfertőzzék a rendszerünket). Viszont a hackerek is veszélyt jelentenek, és a víruselhárító szoftverek nem tudnak eltéríteni egy eltökélt hackert (lásd a negyedik tévhitet). A hackerek megállításához *tűzfalra* van szükség, amely meggátolja őket abban, hogy bejussanak a gépre, és arról is gondoskodnak, hogy ne jussanak ki bizalmas információk a felhasználó engedélye nélkül.

6.1.2 A második tévhit: Nincs a gépemen semmi olyasmi, amit egy hacker kívánhat

A hackerek könnyen megtalálják a számítógépen tárolt bizalmas információkat, mondjuk a személyi és adószámot, netán a bankszámlaszámot, és bárki nevében vásárolhatnak. Az Egyesült Államokban ma a személyazonosság ellopása a legnagyobb mértékben növekvő „fehérgalléros" bűncselekmény. Még ha esetleg semmilyen pénzügyi munkát nem is végzünk a számítógépünkön, azért lehet rajta egy önéletrajz, ami ráadásul még az asztalra is ki van téve, és hogy hívhatnák másként, mint: „Önéletrajz". Az önéletrajzban pedig ott a nevünk, a lakcímünk, hogy hová jártunk iskolába, és hol dolgoztunk eddig. Ezek pontosan olyan információk, amelyek egy hitelkártya vagy egy kölcsön igényléséhez szükségesek. Ha a hackerek hozzájutottak a személyi adataikhoz, különösen a személyi számhoz vagy az adószámhoz, sokféle kárt okozhatnak.

6.1.3 A harmadik tévhit: Csak a nagyvállalatokra és nem az otthon számítógépezőkre mozdulnak a hackerek

Ez egy másik általános tévhit. „Minek bajlódnának velem, amikor mást se csinálok az otthoni gépemen, mint játszok és levelezek?"

A hackerek általában a könnyű prédára lesnek, és az otthoni gépedet lényegesen könnyebb feltörni, mint egy nagy vállalati hálózatot. A hackerek a neten fellelhető számos kész programmal beszivároghatnak bárki rendszerébe. A nagysebességű kapcsolatok különösen sebezhetők, mivel folyamatos kapcsolódásuk során állandó jellegű az IP-címük, amelyhez jóval könnyebb hozzáférni, és beletelik egy időbe, mire egyáltalán észrevesszük, hogy feltörték a gépünket. Ha az otthoni gépünk mindig be van kapcsolva, és nem nézünk rá gyakran, ideális célponttá válhatunk.

Másrészt a nagy cégek kemény pénzeket öltek az információtechnikai részlegeikbe. Igen vállas víruselhárító programjaik és nagyon hatékony tűzfalaik vannak. Más szóval, hozzájuk nehezebb betörni.

6.1.4 A negyedik tévhit: Egy rakás műszaki ismeret kell ahhoz, hogy valakiből hacker legyen

A közhiedelemmel ellentétben nem kell lángésznek lenni ahhoz, hogy valaki betörjön egy gépbe. A hackeléshez tulajdonképpen igen kevés mű-

szaki ismeret is elég, hiszen bármely keresőgép garmadával szállítja a találatokat a „hacking tools" kifejezésre. Ezek az eszközök pár perc alatt letölthetők, még a használati utasítás is ott van mellettük.

6.1.5 Az ötödik tévhit: az internetszolgáltatóm megvéd a vírusok és a támadások ellen, amikor a neten vagyok

Az internetszolgáltatók a legritkább esetben nyújtanak átfogó védelmet, de valamiért a felhasználók azt hiszik, hogy védik őket. Talán próbálja meg, és kérdezze meg a szolgáltatóját, hogy mennyire védenek ők a vírusok és a hackerek ellen! És még ha nyújtanának is némi védelmet, akkor is fel kell tenni a gépünkre egy jó vírusellenes szoftvert.

Hogy miért? Ha fent vagyunk a neten, a vírusok letöltése ellen védtelenek vagyunk, mert a szolgáltatónk valószínűleg csak a leveleket szűri. Ez meg semmilyen védelmet nem jelent egy saját kezűleg letöltött vírus ellen.

6.1.6 A hatodik tévhit: telefonvonalról internetezek, így nincs miért aggódnom a hackerek miatt

Annyi igaz, hogy a nagysebességű felhasználók védtelenebbek egy támadással szemben. A nagysebességű (vagy más néven szélessávú) összeköttetés azt jelenti, hogy mindig (de legalábbis hosszabb időn át) ugyanaz az IP-címünk, így ha a hackerek egyszer megtaláltak, akkor bármikor vissza is jöhetnek.

A jóval lassabb, telefonbehívós hozzáférésnél az IP-cím minden alkalommal más. Ez a véletlenszerű cím okozza azt, hogy a telefonvonalon internetezőkben kialakulhat egyfajta hamis biztonságérzet, ettől azonban a hackerek még ugyanúgy megtalálhatják őket.

Ha telefonos kapcsolatunk van, a hozzánk betörő hacker feltelepíthet egy hátsó ajtós trójait, amely mindig elárulja neki, ha felkapcsolódunk. A trójai, mint egy világítótorony jelzi: „Itt vagyok, gyere és fogj meg". A hackerek így mindig tudják, mikor vagyunk a neten. Az sincs kizárva, hogy a trójait egy e-mail vírus hozza házhoz, vagy egy fertőzött internetes fájllal sikerül letölteni. Ha pedig már beszedtünk egy trójait, teljesen mindegy, hogy nagysebességű a kapcsolatunk vagy csak egy sima behívó.

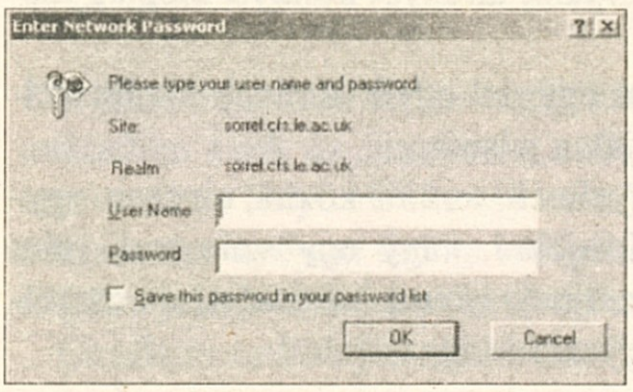
6.1.7 A hetedik tévhit: Macintosh-om van

A Mac-felhasználók gyakran védettnek hiszik magukat, mivel a vírusok többsége a windowsos környezetek ellen készül. Ez azonban nem érdekli a hackert. Az egyik számítógép olyan számára, mint a másik. Nem törődnek azzal, hogy milyen rendszert használnak, csak a nyitott portok érdeklik őket.

Sok Mac-specifikus hackerszerszám érhető el könnyedén az interneten. Ráadásul az új OS X Uunixra épül. A Unix-számítógépek olyan régóta léteznek, hogy a Unixra létező hackerszerszámok nagy része már Macintosh-ra is használható.

6.2 A hackerbiztos jelszó

Mint a legtöbb számítógép felhasználó, feltehetően Ön is bizonyára több jelszót használ – egyet az e-mailjéhez, egyet az online bankügyeihez, egyet a kedvenc e-kereskedőjéhez. Sokaknak tucatnyi, esetleg még több jelszavuk van, és ennyi felhasználói nevet és jelszót igen bonyolult észben tartani. Nagy a kísértés olyan jelszavak létrehozására, amelyekre könnyű visszaemlékezni, például a születési dátumunk, a kutyánk neve vagy más kézenfekvő választás. Aki ezeket választja, az a hackerek kezére játszik. A hackerbiztos jelszó létrehozásában az a kihívás, hogy a lehető legbonyolultabb, tippeléssel ki nem található jelszót válasszuk, amelyet mégsem fogunk elfelejteni.



A jó jelszó segít útját állni a hackerek támadásainak

Íme néhány tipp egy ésszerű jelszó kiválasztásához:

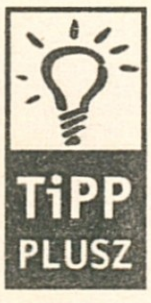
- Kis és nagybetűk, írásjelek és számok kombinációit használjuk.
- Minden azonosítóhoz különböző jelszót használjunk.
- Rendszeresen változtassuk a jelszavunkat. Hogy ne felejtsük el megváltoztatni a jelszót, kössük azt egy eseményhez. Ez lehet például minden hónap elseje, vagy a fizetési nap.
- Legalább hat karakter hosszú jelszót használjunk. Minél több karakterből áll a jelszó, annál nehezebb kitalálni azt.
- Olyan jelszót válasszunk, amelyet könnyű megjegyezni, így nem kell azt leírni.

Elkerülhetjük a megfejthető jelszavak használatát a következő irányelvek betartásával:

- Ne használjunk olyan neveket vagy számokat, amelyek hozzánk kötődnek (pl. születési dátum vagy becenév).
- Semmilyen formában se használjuk a felhasználónevet.
- Ne használjuk a családtagunk vagy a háziállatunk nevét.
- Ne használjuk a „jelszó" szót.
- Ne használjunk semmilyen olyan információt, amelyet könnyű megtudni rólunk. Így ne használjunk rendszámot, telefonszámot, társadalombiztosítási számot, az autónk márkáját, az utca nevét, ahol lakunk stb.

6.2.1 A jelszó fejben tartása

A jelszót mindig memorizáljuk és soha se írjuk le. Vannak módszerek, amelyek segítenek olyan jelszót választani, amelyet könnyű megjegyezni, de nehéz feltörni.



- Használjunk például betűszavakat egy dal egyik sorának kiválasztásával, ahol a szavak kezdőbetűi alkotják a jelszót.
- Válasszunk két rövid szót, amelyeknek semmi közük nincsen egymáshoz, és kombináljuk őket egy írásjellel, vagy egy számmal, mint „moha9pad" vagy „gyors!fal". Használjunk ismert kifejezést, de cseréljük le az „o"-kat nullára, az „i"-ket egyesre és így tovább.

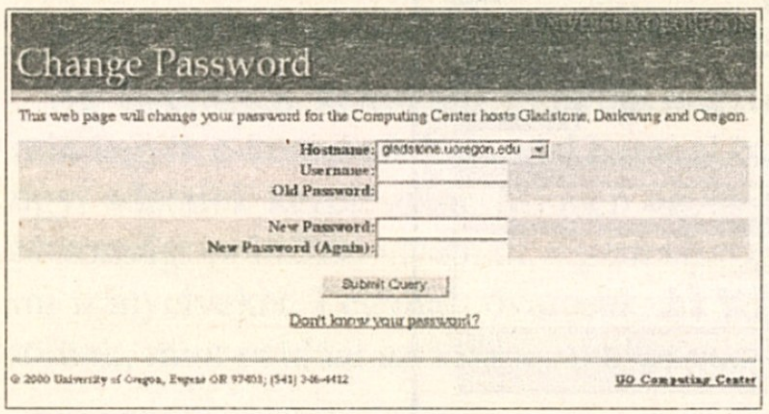
6.2.2 Nyomon követés

Ha úgy érezzük, hogy a rengeteg jelszó fejben tartása túl bonyolult, számtalan módszer létezik azok tárolására. Ezek közül némelyik lehetővé

teszi, hogy a tárolt jelszóhoz akkor is hozzájussunk, ha úton vagyunk, vagy másvalaki számítógépét használjuk.

Jelszótároló szoftver. Számos olyan program létezik, amely lehetővé teszi a felhasználói nevek és jelszavak tárolását, és azt, hogy a felhasználó egyetlen, fejben tartott jelszóval hozzáférhessen ezekhez. Ezen programok némelyike titkosítja a jelszavunkat, így azok fokozottan védettek a kíváncsiskodó tekintetek elől. Az asztali jelszótároló szoftvermegoldások egyik hátránya, hogy nincs hozzáférésünk a tárolt jelszavaikhoz, ha nem a szoftvert futtató gépet használjuk. Ha csak az otthoni gépünket használjuk internetezésre, vásárlásra és banki ügyeinek intézésére, akkor viszont ez a megoldás ideális lehet.

Online jelszótárolás. Rengeteg lehetőség van jelszavunk online tárolására is. Ezek a rendszerek a nap 24 órájában állandó hozzáférést biztosítanak az elmentett felhasználóneveikhez és jelszavaikhoz. Több közülük



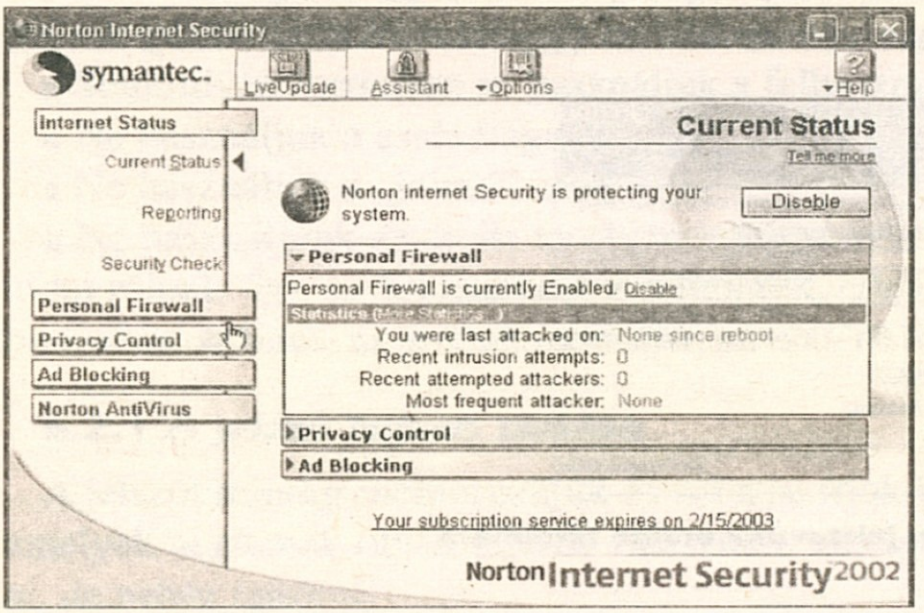
Számos lehetőségünk van jelszavunk online tárolására

128 bites titkosítási technológiát kínál, biztonságban tartva jelszavainkat, miközben azok az interneten utaznak. Bizonyos online tárolóoldalak a szerverükön helyezik el a tárolandó jelszavakat. A biztonság miatt aggódók részére nyújtott online szolgáltatások a felhasználó számítógépén tárolják a jelszavakat, ahol kevésbé valószínű, hogy valaki eléri azokat.

Grafikus online jelszótárolás. Ez a lehetőség megkönnyíti annak a jelszónak a fejbentartását, amely az összes többit védi. A „jelszó" valójában olyan tevékenység grafikus megjelenítésének a sorozata, mit például a mosogatás. Mindössze arra kell emlékezni, hogy milyen sorrendben kell a tevékenységet végrehajtani ahhoz, hogy hozzáférjünk a jelszavunkhoz.

6.2.3 A jelszó biztonságban tartása

Ha választottunk egy nehezen feltörhető jelszót, ügyeljünk arra, hogy a lehető legbiztonságosabban őrizzük azt. Soha ne küldjük el jelszavunkat e-mailben, és ha valaki felhív minket a jelszavunk után kérdezve, ne mondjuk meg. A valódi informatikai személyzetnek már úgyis van jogosultsága ahhoz, hogy hozzáférjen a rendszerünkhöz. Ha egyszer létrehoztuk a tökéletes jelszavunkat, őrizzük azt például a *Norton Internet Security™ 2002*-vel. A Norton Internet Security nélkülözhetetlen védelmet nyújt a vírusok, a hackerek és a bizalmas adatok elleni támadásokkal szemben is. Ez a mindent az egyben programcsomag tartalmazza a hackerek távoltartására a Norton Personal Firewall-t, a személyes információk védelmére pedig a *Norton Privacy Control*-t.



A Norton Internet Security csomag a jelszavunkat is megőrzi

6.3 Az otthoni biztonságról

Az internet, vitathatatlanul meglévő veszélyei ellenére, manapság már sok-sok család életébe bekéredzkedett. A tudatos felhasználó sokat tehet az otthoni számítógép biztonsága érdekében. Nézzük, melyek ezek!

- Ne állítsuk úgy be az e-mail-programokat, hogy önműködően futtassák a csatolmányokat! Legyünk bizalmatlanok az ismeretlen forrásból származó csatolmányokkal!

- Az újabb vírusok képesek arra, hogy olyan e-maileket küldjenek, amelyek látszólag ismerőseinktől származnak. A csatolmányok megnyitása előtt ellenőrizni kell, hogy az valóban az e-mail küldőjétől származik-e.
- Mindent, amit letöltünk az internetről vagy e-mailben kapunk, meg kell vizsgáltatni vírusirtóval! Olyan helyről, amelyben nem bízunk meg, soha se töltsünk le semmit!
- Használjunk állandóan víruselhárítót, és rendszeresen frissítsük a vírusazonosítókat!
- Védekezzünk tűzfallal! A víruselhárító önmagában nem nyújt elegendő védelmet a hackerek ellen.
- A bizalmasság megóvását szolgáló programmal határozzuk meg pontosan, mely webhelyek tárolhatnak információt a tevékenységünkkel kapcsolatban.

6.3.1 Néhány szó az online vásárlásról

Az interneten keresztüli vásárlás nagyon kényelmes, de sajnos nem mindegyik e-kereskedelmi oldal használ biztonságos tranzakciókat pénzügyi adataink kezelésekor. Minden egyes oldalnál érdemes ellenőrizni a biztonsági politikát, valamint a pénzvisszatérítési és magánszféra védelmi irányelveket. Legyünk óvatosak, ha személyes információkat kérnek tőlünk, mint például az adószámunkat vagy a bankszámla-adatainkat.

Az online vásárlás is számos veszélyt rejt magában

Némely e-kereskedelmi oldalnál jelszavas hozzáférést hoznak létre a felhasználó számára. Soha ne használjuk ugyanazt a jelszót, amelyet más hozzáférésnél is alkalmazunk. Soha ne adjuk meg a jelszavunkat kéretlen e-mailekre válaszul, még akkor sem, ha az állítólag az internet-szolgáltatónktól származik. Figyeljünk oda a kereskedelmi oldal URL–jére (Uniform Resource Locator), és bizonyosodjunk meg arról, hogy a megfelelő vállalattal van dolga.

6.3.2 Idegenekkel való érintkezés a hálón

Az internet kiváló lehetőséget nyújt új emberek megismerésére és új dolgok elsajátítására. Mégis elkél az óvatosság. Fogadjunk meg pár tanácsot:

- Amíg nem ismerünk igazán egy új online szereplőt, tartózkodjunk az e-mailtől, a chat-től és a nyilvános helyektől.
- Ne higgyük el mindenkinek, hogy igazat mond a nevével, a nemével, a foglalkozásával és a lakhelyével kapcsolatban. A statisztikák azt mutatják, hogy az online chat-elők többsége nem az, akinek kiadja magát.
- Legyünk óvatosak abban is, hogy milyen és mennyi személyes információt adunk meg magunkról olyanoknak, akiket nem ismerünk.
- Nem kell minden vendégkönyvet aláírnunk, ez csak kéretlen leveleink számát növeli.
- Ha nyilvános üzenetküldő rendszert használunk, fontoljuk meg egy másik identitás használatát.

6.3.3 Online biztonság – gyermekeknek

Ha Önnek internetező gyermekei vannak, egész biztosan aggódik a biztonságukért, és szeretné őket megkímélni az információs szupersztráda veszélyeitől. Igaz, hogy az online tartalom nagy része nem veszélyes rájuk nézve, de a felnőtteknek szóló vagy más módon nem kívánatos tartalom is könnyen elérhető a számukra. Sajnos, éppen ezeken a tartalmakon keresztül szeretnék a gyermekeket elérni veszélyes és illegális okokból.

Alább felsorolunk néhány veszélyforrást, amelyek a gyermekeket fenyegetik internetezés közben.

- **Helytelen tartalom.** A gyermek szexuális, gyűlöletkeltő vagy veszélyes, illetve illegális cselekedetre bátorító tartalom közelébe kerülhet.

Egy kutatás eredményei alapján elmondhatjuk, hogy a 10-17 éves gyermekek 25%-a kapott már nemkívánatos szexuális tartalmú képeket.

- **Jogi és pénzügyi kérdések.** A gyermek elcsábulhat, és megadhatja a hitelkártyaszámot, amelynek pénzügyi következményei lehetnek Önre nézve. Esetleg rábeszélhetik, hogy más személyes jogait sértő módon viselkedjék, amely jogi problémákat vethet fel a család számára.
- **Magánszféra.** A gyerekek, még a tinédzserek is, hajlamosak kiadni privát információkat. Személyes információk, mint név, cím, életkor, nem, családi részletek könnyen rossz kezekbe kerülhetnek. Még ha egy hiteles szervezet kéri is ezeket az információkat, oda kell figyelni a gyermek magánszférájának a védelmére.
- **Technikai kérdések.** A gyermek véletlenül beengedhet a számítógépbe vírust, férget, trójai falovat, vagy más veszélyes fenyegetést, amikor megnyit egy csatolmányt vagy nem biztonságos helyről tölt le információt.

6.3.4 Mit tehet a felnőtt?

Igaz, hogy internetes fenyegetések léteznek, de ennek nem szabad megakadályoznia bennünket az internet kínálta lehetőségek élvezetében. Szerencsére számtalan eszköz áll a szülők rendelkezésére, hogy megvédjék önmagukat és gyermekeiket az online veszélyektől.

Beszéljünk a gyermekkel! Az első teendő, hogy tudatosítsuk a gyerekben: az online állapot nyilvánosságot jelent. Az internetes veszélyek nagy része hasonló ahhoz, mintha egy idegennel lennénk négyszemközt, és a gyerekeknek meg kell érteniük, hogy ha nem ismerik személyesen azt, akivel érintkeznek, az olyan, mintha idegen lenne az illető.

Készítsünk „internetezési szabályokat". Legyen a gyerek tisztában azzal, hogy mely oldalakat szabad látogatnia és melyek az internet használatának szabályai. Tudatosítsuk benne, hogy mire kell vigyáznia. Figyelmeztessük, hogy ne adja meg a jelszavukat senkinek, még akkor sem, ha az illető azt állítja, hogy az internet-szolgáltatónak dolgozik. Az internet-szolgáltató sosem kéri az előfizető jelszavát. Ne engedjük, hogy a gyerek „beszélgető csoportokhoz" (chat) csatlakozzon, vagy legalább figyeljünk oda rá, amikor ilyen módon beszélget az interneten keresztül. Csak moderált és jó nevű szervezet által fenntartott beszélgető csoporthoz engedjük őt csatlakozni.

Használjuk saját célunkra a technológiát! Figyeljük meg a gyermek bejövő és kimenő leveleit. Ismerjük meg a „cyber barátait", mint ahogy a hús-vér barátait is ismerjük. Nézzük meg gyakran a böngészőben található *Előzményeket,* ahol láthatjuk, mely weboldalakat és milyen gyakran látogatott meg csemeténk.

6.3.5 Ötletek a széles sávon internetezők védelméhez

Azt gondolhatnánk, hogy az egyszerű otthoni számítógép-használó a legkevésbé sem érdekli a hackereket. A legtöbbjük persze nem is a magánjellegű adatokra kíváncsi, inkább az hajtja, hogy egy kevéssé védett otthoni gép mögött megbújva támadhasson másokat a gép gazdájának tudta nélkül.

1. **Tartsuk távol a gazfickókat!** – Ha tűzfal nélkül internetezünk, védtelen vagyunk a többi internetezővel és a rosszindulatú hackerekkel szemben. Bár egy állandóan élő internetkapcsolat nyilvánvaló előnyökkel jár, ez a kapcsolat állandóan nyitva áll a hackerek előtt is. A tűzfal használatával távol lehet tartani a hackereket, és biztonságban böngészhetünk anélkül, hogy aggódnunk kellene a számítógépen levő információ biztonságáért.
2. **A letöltések dilemmája** – A hackerek a rosszindulatú programokat ártatlannak tűnő fájlokba rejthetik el. Bár a szélessávú kapcsolat egyik legnépszerűbb felhasználási módja a letöltés, feltétlenül vizsgáljuk meg letöltés előtt a fájlokat, és tartsuk napra készen a víruselhárító szoftvert. Így védve lehetünk a legújabb vírusok ellen is, és elkerülhetjük a veszélyes tartalmak letöltését.
3. **Zárjuk be az ajtót!** – Használjuk a józan eszünket az interneten is! A folyamatos kapcsolat nagyon jó az internetezésre, de egy kicsit hasonlít ahhoz, mintha mindig tárva-nyitva állna a lakásunk ajtaja. Ha nem internetezünk, zárjuk be az ajtót, azaz bontsuk a kapcsolatot!
4. **A jelszavas védelem** – Védjük jelszóval a számítógépen tárolt bizalmas anyagokat! Használjunk olyan ellenálló jelszót, amelyet nehéz feltörni (lásd még: hackerbiztos jelszó, ugyanebben a fejezetben).
5. **Ellenőrizzük a védelmet!** – Ha biztosak akarunk lenni abban, hogy megfelelő a számítógépünk védelme, használjuk a **www.symantec.com/securitycheck/** címen található ingyenes *Symantec Security Check*-et!

7 A nagy biztonsági csomag

Könyvünk utolsó fejezetében még egyszer összefoglaljuk azokat az ismereteket, amelyek a PC 100 százalékos védelméhez szükségesek, és egy nagy „biztonsági csomagot" is átnyújtunk olvasóinknak.

A nagy biztonságnak persze megvan az ára: minél szigorúbbak a Windows, az Internet Explorer, valamint a tűzfal biztonsági beállításai, annál kevesebbet engedélyez az operációs rendszer.

Ez a kárt okozó kódok futtatása esetében ugyanúgy érvényes, mint ezek hasznos változataira. Különösen az úgynevezett ActiveX-Control programok érintettek, amelyeken keresztül sok bővítmény és plug-in is dolgozik az Internet Explorer számára. Ezek az irányítóelemek aktív tartalommal ruházzák fel az internetoldalakat. Mivel ezzel tárcsázóprogramként is visszaélhetnek, először is ajánlatos az összes Active-X elem kikapcsolása. Azonban így is számolnunk kell az egyes weboldalak esetében azzal, hogy az oldal nem teljes egészében jelenik meg, vagy nem működik. Ebben az esetben legalább időlegesen vissza kell állítanunk az Internet Explorerben a biztonsági beállításokat. Néhány internetoldal-üzemeltető, mint például az online bankok nyomatékosan felhívják arra a figyelmünket a böngészőben, hogy a probléma valószínűleg az Internet Explorer hibás beállításával függ össze. Ezt azonban amúgy is mindig észben kell tartanunk.

A biztonsági beállításokat a leggyorsabban a *SecureIE* eszközzel állíthatjuk vissza, amely egyébként CD-mellékletünkön is megtalálható.

Indítsuk el a programot előzetes telepítés nélkül közvetlenül a CD-ről. Átmenetileg válasszuk a *Közepes biztonság* (*Mittlere Sicherheit*) szintet, és végezzük el a hozzá tartozó beállításokat az *IE konfigurálása/OK/Nem/Ablak bezárása* (*IE konfigurieren/OK/Nein/Fenster schliessen*) gombokon keresztül.

Végezzük még el az interneten az eddig nem működő kívánt akciókat, és gondoljunk arra, hogy ezek után ismét emeljük fel a biztonsági beállítások szintjét.

Ezen kívül még a *Shields-Up* online biztonsági ellenőrzés ajánlott

(**http://grc.com/x/ne.dll?bh0bkyd2**). Ennek az eszköznek segítségével megtudhatjuk, hogy milyen formában és melyik porton keresztül támadható meg a számítógépünk. Ez az internetoldal ugyan angol nyelvű, de *Steve Gibson* biztonsági szakember a kezdők számára is érthetően elmagyarázza a tennivalókat (*First time users*). A biztonsági elemzések eredményeitől függően különböző tippeket kaphatunk azzal kapcsolatban, hogy miként tömhetjük be a biztonsági falon támadt lyukakat.

Nagy biztonsági programgyűjtemény

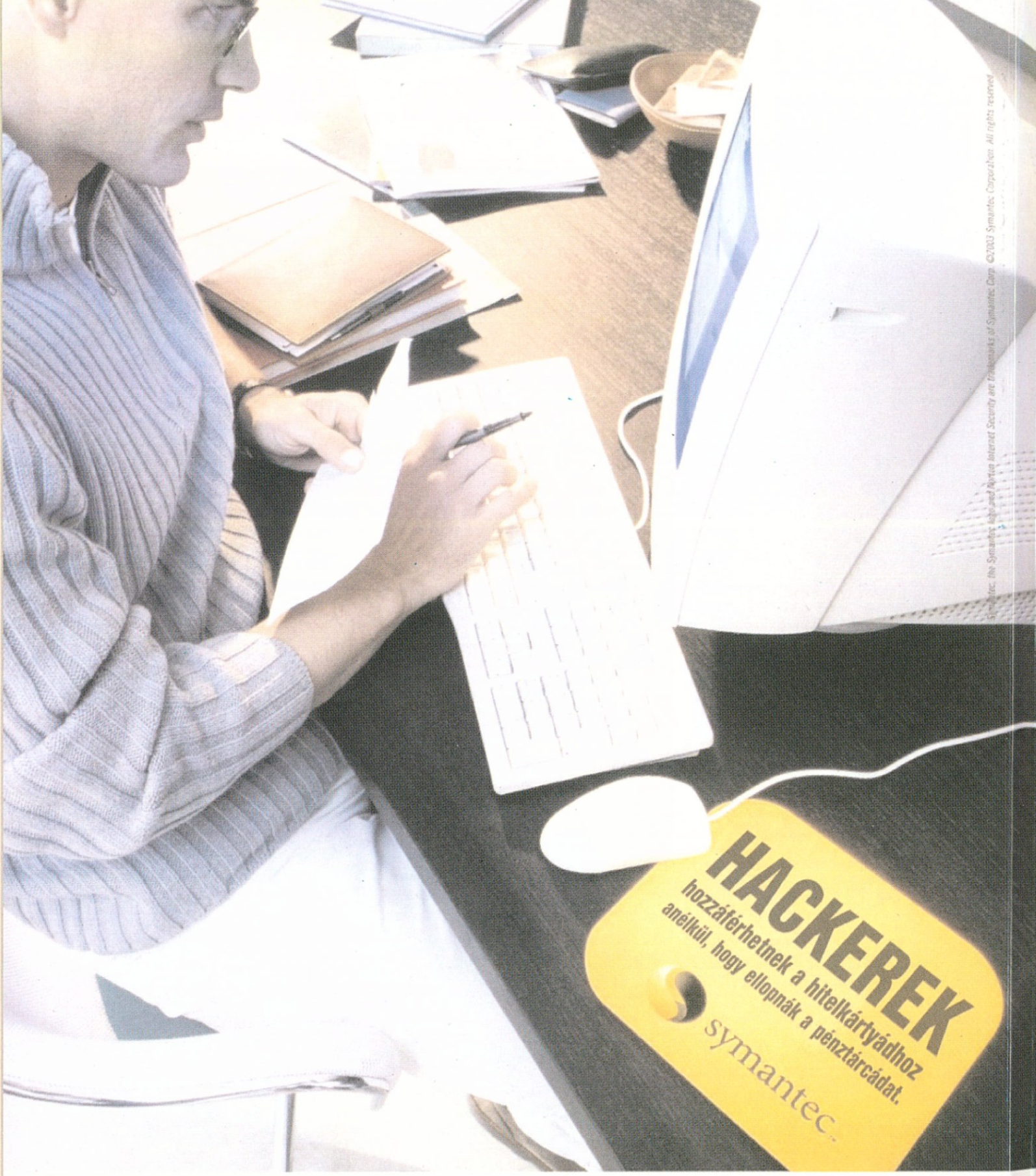
Program	Internetcím	Megjegyzés
Vírus elleni védelem		
AntiVir PE	www.free-av.com/	Az AntiVir Pesonal Antivírus program vírusőre folyamatosan ellenőrzi a letöltéseket az Internetről.
Quick Heal X-Gen	www.quickheal.com/	Ez a vírusszkenner a tömörített fájlokat is átvizsgálja, és különleges védelmet biztosít az Office 2000/XP dokumentumok számára.
VCatch Basic	www.vcatch.com/	A Vcatch Basic vírus-szkenner program az egész e-mail forgalmat, valamint a webletöltéseket is átvizsgálja.
PC Cillin	www.trendmicro.com/	A PC Cillin nemcsak a vírusokat hárítja el, hanem szabályozható biztonsági szintekkel ellátott tűzfalallal is szolgál.
BugBear Decrypter	www.av-test.org/	A BugBear Decrypter megnyitja a Keylogger-protokollt, amelyet a Win32=Bugbear.B állított elő, és kiszabadítja a kikémlelt jelszavakat.
Tűzfalak		
ZoneAlarm	www.zonelabs.com/	A ZoneAlarm teljes értékű, ingyenes tűzfal, amely megbízható védelmet nyújt számítógépünknek az internetes támadások ellen.

Program	Internetcím	Leírás
Sygate Personal Firewall	www.sygate.com/	Ez a tűzfal átfogóan konfigurálható és az összes ki- és bemenő kapcsolatot megbízhatóan felügyeli.
Kerio Pesonal Firewall	www.kerio.com/	A Kerio Personal Firewall programban három biztonsági szint közül választhatunk, amelyek megvédik számítógépünket a web és a hálózat támadásai ellen.
Outpost Firewall Pro	www.agnitum.com/	Az Outpost állandó védelmet nyújt: a tűzfalrendszerünket védi hackerek ellen, sőt a nem kívánatos reklámokat is meggátolja.
Anti-Spyware		
Advanced Anti Keylogger	www.anti-keylogger.net/	Az Advanced Anti Keylogger a kém–szoftverek és az olyan programok ellen véd, amelyek a billentyűzeten beadott adatokat jegyzik fel.
XP-AntiSpy	www.xp-antispy.org/	Az XP-AntiSpy megakadályozza, hogy a Windows kérdezés nélkül információkat küldjön át a Microsoftnak.
CookieCooker	cookie.inf.tu-dresden.de/	A CookieCooker az úgynevezett eldobható mail-címeken keresztül nyújt védelmet, hogy érdeklődési körünket és szokásainkat ne lehessen kikémlelni.
WinPatrol	www.winpatrol.com/	A WinPatrol az összes nem kívánatos programot eltávolítja, amelyek a Windows indításakor automatikusan töltődnek.
Ad-aware	www.lavasoftusa.com/	Az Anti-Ad és az Anti-Spy programok klasszikusa az összes ké-eszközt eltávolítja a számítógépünkről.
SpyBlocker	spyblocker-software.com/spyblocker/	Az Ad-adware kiegészítéseként ajánlott a Spy-Blocker.
SpyCop	spycop.com	A Spy-Cop arra specializálódott, hogy a Keylogger és a trójai falovak általi fenyegetést felfedezze.

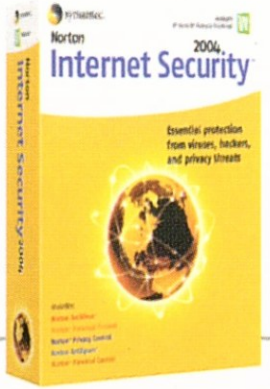
Program	Internetcím	Megjegyzés
Trójai faló elleni védelem		
Pest Patrol Home	www.pestpatrol.com	A Pest Patrol a trójai falovak, a kémprogramok, a jelszókémlelők, a hackereszközök, az adware-k, a billentyűzetkémlelők és a Denial-of–Service támadások ellen nyújt védelmet.
TrojanCheck	www.trojancheck.de	A TrojanCheck olyan program, amellyel ismeretlen trójai falovat is könnyedén felismerhetünk és megsemmisíthetünk.
TrojanHunter	www.misec.net	A TrojanHunter eltávolítja azokat a trójai falovakat a számítógépünkről, amelyek segítségével mások átvehetnék az uralmat a PC-nk felett.
Kódolás		
ArchiCrypt Live	www.archicrypt.com/textACL.htm	Az ArchiCrypt Live egy valós idejű kódolás, amely segítségével a felhasználó három lépésben hozhat létre kódolt meghajtót.
Krypter 2002	www.babe.de/	A Krypter 2002 egy gyors program, amellyel bármilyen típusú fájlok és komplett kényvtárak is hozzáférhetetlenné tehetők.
CompuSec PC Security	www.sofotex.com	Jelszavas védelem a számítógépen: a CompuSec PC Security védi rendszerünket
PC-Lock	www.pclock.net	Megbízható hozzáférési védelmet nyújt az ingyenes PC-Lock program, amely az össze billentyűkombinációt zárolja.
Global Safe Disk	www.globalsafedisk.com	Bizalmas adataink nagyfokú biztonságát nyújtja a Global Safe Disk kódoló program, 512-bites alapon.
Nyom/identitás eltüntetése		
Internet Anonym 5	www.steganos.com	A Steganos cég Internet Anonym 5 programjával gombnyomásra anonímként szörfölhetünk a világhálón és a veszélyes webtartalmak elől is védettek vagyunk.

Program	Internetcím	Megjegyzés
ClearProg	www.clearprog.de	A ClearProg kitörli nyomainkat az Internet Explorerben, valamint az Opera és a Netscape böngészőkben is.
Backup-programok		
Z-D Backup	www.bsx.de	A Z-D Backup egyszerűen , gyorsan és megbízhatóan menti el az adatokat bármelyik célmeghajtóra, valamint CD-R-re vagy szalagra. Még teljes partíciókat is átvesz egyetlem backup-fájlba.
Backup Maker	www.ascomp.de	A Backup Maker adatokat biztosít, hálózatban is alkalmazható és ezért cégek számára is ajánlott.
Smart Backup	www.jam-software.com/smartbackup/	A SmartBackup segít az adatvédelmi okokból fontos adatok megtalálásában, és így alacsonyan tartja a backup program idejét.
Jelszófelügyelet		
1 Password	www.shmoo.com/mail/fw1/apr99/msg00862.html	Csak egy jelszó megjegyzésére lesz szükség: az 1Password-adatbank hozzáférési jelszavára. Az összes többti ezzel az eszközzel felügyelhetjük.
Password Safe and Repository	www.passwordsafe.de/	A Password Safe kényelmes megoldás a jelszavak és a TAN–blokkok felügyeletére.
Passwort Depot	www.softguide.de	A Password Depot minden jelszót egyetlen jelszólistában tárol, ahol a drag and drop művelettel rendelkezésünkre állnak.
Spam-megsemmisítők		
EMC	www.emc.com	A E-mail Control tömeges vagy nagyméretű csatolt fájlos üzenetek ellen véd.
SpamEater Pro	www.hms.com/spameater.asp	A SpamEater Pro az automatikus szűrőszabályokon keresztül megakadályozza a nemkívánatos e-mailek letöltését.

Program	Internetcím	Megjegyzés
Spamihilator	www.spamihilator.com	A Spamihilator megakadályozza a nem kívánt üzenetek letöltését, és minden mail programmal együttműködik.
MailTalkX	www.softbytelabs.com/MailTalkX/	A MailTalkX egy spam szűrő és e-mail program, amely több postafiókot felügyel és véd a spam-ek ellen.
SpamNet	www.spamnet.org	Az Outlook-Plug-In SpamNet a junk-mail áradatot redukálja úgy, hogy a nagy Anti-Spam-Community mail-eket spamként jelöli
DataDestroyer	www.spychecker.com/program/datadestroyer.html	A DataDestroyer úgy törli a kényes adatokat, hogy azok többé nem állíthatók vissza.
Secure Eraser	www2.neweb.ne.jp/wd/morimoto/en/diskeraser/	Az öt jól bevált szabvány használata által a Secure Eraser végérvényesen törli a merevlemezről a kényes fájlokat .
File Wiper	home.att.net	A File Wiper biztonságosan törli a fájlokat a merevlemezről: a szabad memóriahelyet is többször felülírja.
Biztonság		
SecureIE	www.secureie.com	Amit egyébként körülményesen kézzel kell beállítanunk, a SecureIE teljesen automatikusan elvégez: biztonságossá teszi az Internet Explorert



Magyar nyelvű változat
Vírusvédelem
Személyes tűzfal
Magánszféra védelem
Szülői kontroll
Spamszűrés



1490 Ft

9 789637 639340

Get Protected.

További információ: **www.symantec.hu**