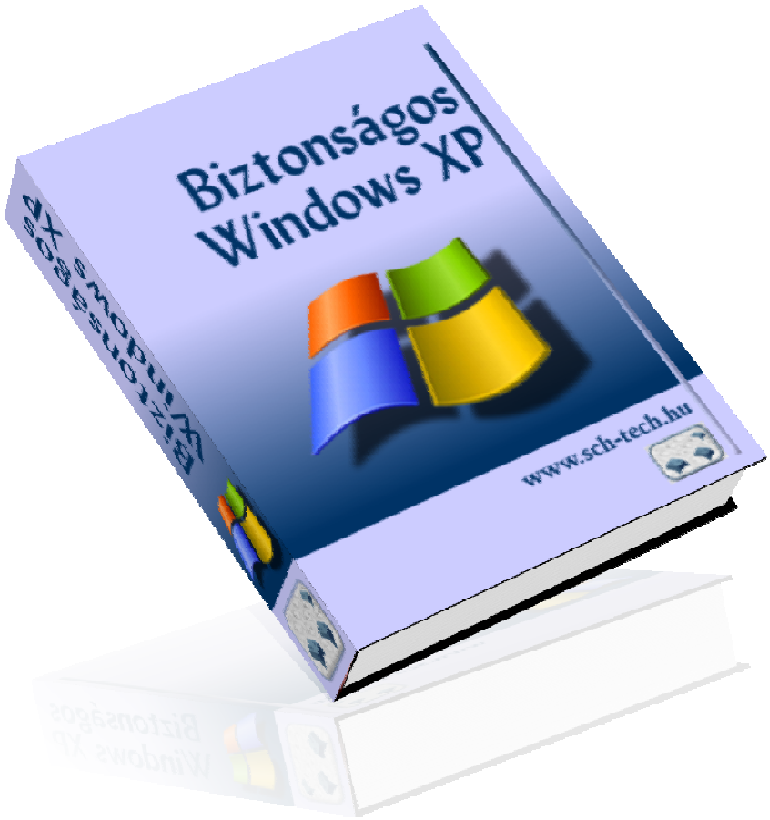
Biztonságos Windows XP

Tippek a Windows beállításához

www.sch-tech.hu



Biztonságos Windows XP – Tippek a Windows beállításához

ISBN 978-963-06-4530-0

http://www.sch-tech.hu

Tartalomjegyzék

Előszó

Kedves Olvasó!

Kérlek, nézd el nekem a tegező hangnemet, de sokkal jobban szeretek közvetlen módon társalogni azokkal, akik megkérnek, hogy segítsek nekik valamiben. Ha ez a segítség „csak" annyiból áll, hogy elmondom, miképpen tudod megbízhatóbbá tenni az otthoni számítógépedet, akkor is szeretem azt a magam módján felvezetni. Ennek fényében szeretnék röviden bemutatkozni.

Már a középiskolában (1990 környékén) elkezdtem érdeklődni a számítógépek iránt, de teljes erővel a diplomám megszerzése óta (1996) foglalkozom az informatika világával. Sok területéből leginkább oktatással, honlap készítéssel (design és programozás) valamint hardver- és szoftverkarbantartással töltöm az időmet. Az utóbbi években azonban nagyon megnőtt azon ismerőseimnek – illetve az ismerőseim ismerőseinek – a száma, akiknek már szinte napi problémáik vannak a számítógépükkel. Mindez az egyre jobban terjedő Internetnek „köszönhető". Amíg csak önálló, elszigetelt számítógépek voltak, sokkal kevesebb feladat volt a karbantartás területén.

A rengeteg felmerülő gondot már nem lehet normális időben kezelni, ha az ember szeretne némi időt a családjával is eltölteni. ☺ Ezen a felismerésen felbuzdulva döntöttem eme útmutató megírása mellett, hogy Te magad önállóan is képes legyél megvédeni a számítógépedet és megelőzni a nem kívánt kellemetlenségeket.

Kívánom, hogy sikerrel alkalmazd a segédletben található információkat!

Üdvözlettel,
Scheib János

http://www.sch-tech.hu

Védd meg a számítógépedet a behatolóktól

A számítógép biztonsága az egyik legfontosabb kérdés a mai elektronikus világban. A Windows operációs rendszer ellen irányuló vírusok és rosszindulatú programok sokasága miatt mindenképpen megelőző lépésekre van szükség számítógéped védelme érdekében. Manapság a vírusok és férgek aktívan támadják a számítógépeket, hogy felhasználói tevékenység nélkül is megfertőzhessék azt. Ha egy vírus vagy féreg bejutott egy rendszerbe, a fertőzött számítógép könnyen terjesztő központtá válhat, ami egyéb kellemetlen dolgokat vonhat maga után. Ha a számítógéped nem védi az internet-kapcsolatát, akkor potenciális veszélynek vagy kitéve!

Ebben a fejezetben megmutatom, hogyan tudod tesztelni a gépedet és megnézni, mennyire sebezhető is valójában. Utána megtudod, hogyan állíthatsz be tűzfalat és azt is, hogyan kapcsolj ki olyan szolgáltatásokat, amikre alapesetben nincs szüksége a Windows XP-nek, és nagyon megnövelik a megfertőződés kockázatát. Végül pedig lesz néhány szó a vezeték nélküli kapcsolatok biztonságáról is, mivel ez egy meglehetősen aktuális téma.

Ha már lezártad a számítógépedet kívülről, akkor is lehet még nyitva néhány út a géped felé, amit szándékosan nem akarsz bezárni. A távoli kapcsolatoknak szükségük van néhány nyitott kapura (**port**), amiken keresztül csatlakozni tudsz a gépedhez távolról. Például, ha szeretnél fájlokat másolni az otthoni hálózatodon (a gyerek gépe és a Te géped között), akkor szükséged van a Microsoft Network Kliens engedélyezésére. Ez esetben viszont van egy támadási pont a rendszereden, ami ellen védekezned kell. Hogy szembeszállj ezzel a sebezhetőséggel, hallasz majd a különböző felhasználói fiókokról, jelszavakról és jogosultságokról is.

port

A port a számítógép egy bejárata/kijárata. A TCP/IP hálózati kommunikációs nyelvben minden számítógépnek 65535 portja van. Ezeken a kapukon keresztül tudnak a számítógépek (programok) egymással adatot cserélni. Ebből a rengeteg kapuból csak néhánynak van kötött szerepe, ezek is inkább csak megegyezés alapján. Talán a legismertebbek a web-kiszolgálók. Ha egy címen (egy interneten lévő gépen) valaki a 80-as portról kér adatot, azt az adott gépen a web-szerver fogja lekezelni és kiszolgálni vagy nem történik semmi, ha nincs azon a gépen web-szerver, ami figyelné a 80-as portot.

Mennyire sebezhető a rendszered?

A számítógéped fontos információk tárháza. Lehetnek olyan kényes adatok is a gépeden, amiket nem szeretnél az egész világnak megmutatni. Családi fotók, személyes dokumentumok és gazdasági információk majdnem minden számítógépen megtalálhatóak. Ha egy vírus, vagy támadó hozzáfér a gépedhez, akár évek munkáját vagy emlékeit is kitörölheti vagy ellophatja. Essünk hát neki, hogy miket is kellene megvizsgálnod a gépeden…

Teszteld az internet-biztonságodat

Ha egy program adatokat akar küldeni egy távoli számítógépnek, azt annak a gépnek egy adott portjára (lsd. fent) küldi. Ha a távoli gépen egy konkrét program figyeli azt a portot, akkor feldolgozza az oda érkező adatokat. Ez így rendben is van, csak sajnos a programok nem mindig így működnek. ☹ A szoftverek (sem) tökéletesek és néha olyan adatokat küldenek, aminek a fogadására nincsenek felkészítve, ezáltal mindenféle hibákat okoznak. Többek között egy távoli támadó is ezt használja ki, hogy csatlakozzon a gépedhez és parancsokat futtasson rajta. Ezt a típusú támadást **exploit**-nak (kiaknáz, kihasznál) nevezi a szakzsargon.

A számítógéped védelme érdekében **a nem használt portokat** lehetőleg **tartsd zárva** és csak a ténylegesen használt kapukat nyisd meg! A jövőbeni támadásoknak sincs esélyük bejutni egy lezárt bejáraton és csak a nyitott kapukat figyelő programok biztonsági réseit kell folyamatosan foltozgatnod. A portok lezárását **Firewall** (tűzfal) programmal tudod megvalósítani, melyről egy későbbi szakaszban lesz szó.

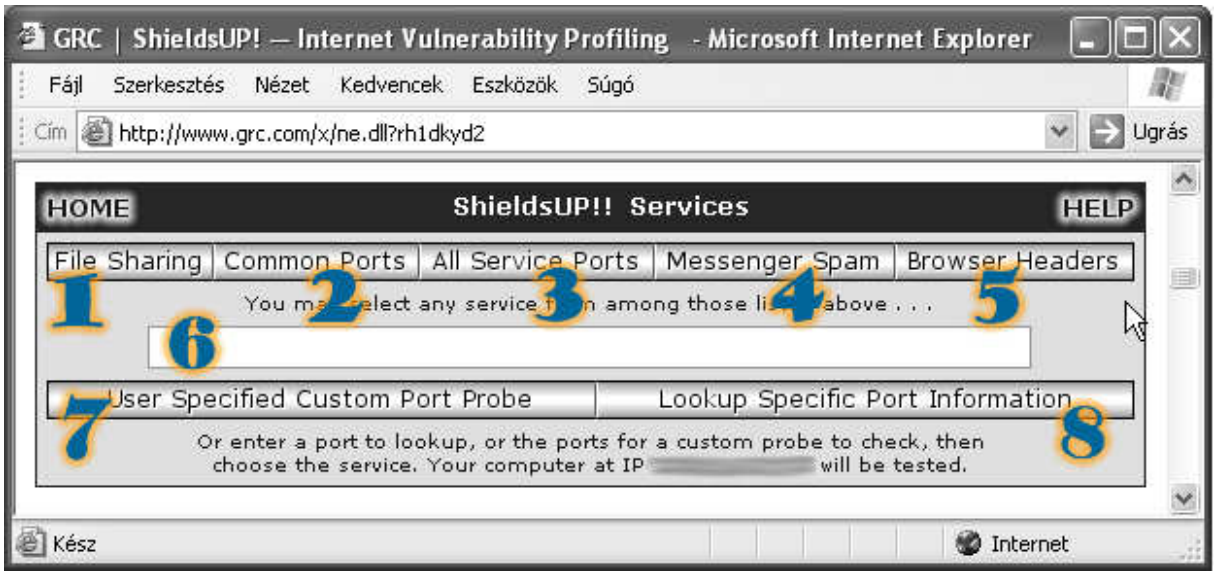
Az Interneten található néhány szolgáltatás, amelyek segítségével letesztelheted, mennyire nyitott a számítógéped.

- **Symantec Security Check** http://security.symantec.com
  Nálam sajnos a naprakész CA eTrust vírusirtót nem érzékelte. Azt mondta, nincs vírusirtóm és mindenképpen rá akart beszélni a Norton Antivirus megvásárlására. Szóval odafigyelve értékeljük a riasztásait…
- **Gibson Research ShieldsUp!** http://www.grc.com
  Igen egyszerű, jó felületet ad gépünk teszteléséhez! Nézzük csak meg, milyen szolgáltatásokat nyújt ez az oldal.

1. ábra: Gibson Research honlapja

A ShieldsUP menüpont kiválasztása után tájékoztat, hogy milyen próbálkozások lesznek, és ha esetleg használsz valamilyen tűzfalat, akkor ott

milyen bejegyzések várhatóak. Ezen az oldalon találsz egy „Proceed” gombot, ami továbbvisz a tényleges tesztelő oldalra. A vizsgálati lehetőségek leírását alább találod.



2. ábra: A GRC szolgáltatási listája

1. File Sharing
   Itt lehet tesztelni, hogy a Windows-os fájlmegosztás elérhető-e kívülről a számítógépünkön.
2. Common Ports
   A leggyakrabban használt, konkrét portokat lehet vele letesztelni.
3. All Service Ports
   Az első 1056 IP portot teszteli külső elérhetőség szempontjából.
4. Messenger Spam
   Ha fut a gépeden a Messenger szolgáltatás (nem MSN), és nincs védve a hozzá való port, akkor kapsz egy felugró ablakot. Ha az bejött, no, az nem jó jel! Le kellene állítanod a Messenger szolgáltatást, ha nem akarsz hamarosan áldozattá válni.
5. Browser Headers
   Megmondja, hogy a böngésződ milyen információkat árul el rólad bármilyen weboldalnak.
6. Port numbers
   Ebbe a beviteli mezőbe írhatsz tetszőleges port számokat a következő két művelet végrehajtásához.
7. User Specified Custom Port Probe
   Felhasználó által megadott port tesztelése. Ha a fenti beviteli mezőt üresen hagyod, akkor kapsz néhány mintát, hogyan írhatsz be port számot.

8. Lookup Specific Port Information
   A fentebb megadott port számról nyújt részletes információt.

Frissítsd a számítógépedet

A Windows XP egy nagyszerű operációs rendszer, de nem tökéletes. A hibáit folyamatosan fedezik fel a leleményes kísérletezők, és ezeket kihasználva megpróbálnak bejutni a számítógépedbe. A Microsoft havonta ad ki frissítéseket (szervizcsomagokat) a szoftvereihez, és ha veszélyes résre derül fény, annak a kijavítását azonnal közzéteszik. Ezek alapján tehát mindenképpen érdemes gyakran – hetente többször – ellátogatnod a Windows frissítő honlapra (http://www.windowsupdate.com).

Sokkal **jobb megoldás** azonban, **ha bekapcsolod az automatikus frissítés szolgáltatást** (Vezérlőpult > Automatikus frissítések), mert akkor biztos, hogy nem maradsz le semmilyen fontos csomagról. Erre viszont csak akkor van lehetőséged, ha már **legalább** a kettes szervizcsomagot (SP2 – Service Pack 2) feltelepítetted a Windows-odra. Érdemes feltenni, mert általa valóban nagyon megnő a Windows XP biztonsága.

Tűzfalak

Mostanra már talán rájöttél, hogy micsoda „vándorlás” folyhat (folyik) a számítógépedben, ha az internetre kapcsolódsz. Sokan megpróbálnak hozzáférni a gépedhez és ennek megelőzésére bizony az előzőekben megismert kapukat be kell zárnod! **A portok lezárásához** egy úgynevezett **tűzfal** (firewall) **programra van szükséged.**

A tűzfal program a beállításaitól függően védi a számítógéped portjait. Ha egy külső behatoló próbál bejutni a gépedbe egy be nem foltozott résen keresztül, akkor lehet, hogy a tűzfal program az adott porton minden kommunikációt blokkol és e miatt a támadó nem kap semmilyen választ, mintha a számítógéped ki lenne kapcsolva.

A Windows XP SP2-es verziója már rendelkezik beépített tűzfal programmal. A legtöbb tűzfal programnak telepítéskor már olyan az alapbeállítása, amely a lehető legtöbb védelmet nyújtja számodra. Ilyenkor szinte minden port blokkolva van és neked kell a számodra szükséges kapukat megnyitnod.

A Windows beépített tűzfala

A Windows tűzfala alapállapotban nincs bekapcsolva, bár ezt a telepítés után rögtön jelzi is és a legtöbben ekkor be is kapcsolják. Célszerű azzal kezdeni a hálózatos használatot, hogy bekapcsolod az alábbi módon:

- Start menü > Futtatás. Írd be, hogy **firewall.cpl** és kattints az OK-ra.
- A megjelenő ablakban jelöld ki, hogy **Bekapcsolva** és kattints az OK-ra.
- Még egyszer kattints az OK-ra és már készen is vagy.

Miután bekapcsoltad a tűzfalat, próbáld ki az összes használni kívánt programodat (böngésző, levelező, csevegő, stb.). Ha esetleg valamelyik nem működik, akkor konfigurálnod kell a tűzfaladat.

Az a jó, ha nem tud minden program kommunikálni, hiszen éppen ezért aktiváltuk a tűzfalat. **Tényleg csak azokat a programokat engedélyezd, amit használni szeretnél!** Csak úgy, az egyszerűség kedvéért NE adj hozzá minden programot és portot, ami csak felmerül. Az SP2 óta a Windows tűzfala kétféleképpen is beállítható. Hozzáadhatsz egy tetszőleges portot, amit szeretnél megnyitni, vagy talán egy könnyebb mód, ha felveszed a használni kívánt programot az engedélyezettek közé.

- Nyisd meg a tűzfal-beállító panelt. Start menü > Futtatás. Írd be, hogy **firewall.cpl** és kattints az OK-ra.
- A megjelenő párbeszédpanelen kattints a **Kivételek** fülre.
- A bepipált alkalmazások mutatják, hogy jelenleg melyek használhatják az internetet. Javaslom, hogy minden olyan bejegyzés elől vedd ki a pipát, amit nem feltétlenül kell használnod.
- Új program felvételéhez nyomd meg a **Program hozzáadása** gombot. Az ott megjelenő listából válaszd ki a programot, vagy ha nincs rajta, akkor a **Tallózás** gombbal keresd ki az állományt.
- Az így felvett programnál már csak azt kell ellenőrizned, hogy a pipa bent van-e előtte és kattinthatsz is az OK gombra.

A Windows Tűzfal olyan beállításokat is tartalmaz, melyek megszabják, hogyan viselkedjen a számítógéped szabványos hálózati üzenetek érkezésekor (pl.: hálózat, elérhetőség tesztelése alkalmával). Mindezt az előbb használt párbeszédpanel **Speciális** fülén lévő **ICMP** kategória **Beállítások…** gombja alatt találod. Ha minél jobban rejtve szeretnéd tudni a számítógépedet, akkor érdemes az ICMP alatt található összes bejegyzésnél kivenni a pipát.

Egyéb szoftveres tűzfalak

Sok szoftverfejlesztő készít tűzfal programot a Windows alá. Szinte mindegyik ilyen programnak van ingyenes, alapszolgáltatásokat nyújtó és fizetős, komplex internet-biztonsági csomagjuk.

Ezek finomhangolása és használata néha nem annyira egyszerű, mint ahogy egy egyszerű felhasználó elvárná. Sajnos olyan sok variációs lehetőség van, hogy az bőven megtöltene egy külön könyvet, ezért itt nem is foglalkozom vele önállóan. Az alábbiakban felsorolok néhány közismert verziót:

- Comodo (http://www.personalfirewall.comodo.com)
- ZoneAlarm (http://www.zonealarm.com)
- Outpost (http://www.agnitum.com/products/outpostfree/index.php)

- Ashampoo (http://www.ashampoo.com)

A fent említettek mindegyike otthoni használatra ingyenes és jól működő tűzfal. Véleményem szerint azonban jobban járunk egy router beüzemelésével (lsd. következő alfejezet).

Fizikai tűzfal

Manapság szinte minden, internetet elérő háztartásban több számítógép is található. Ezek eredményeként nagyon sok helyen használnak egy routernek nevezett hálózati eszközt az internet-kapcsolat megosztására. Az ilyen routereknek az az előnye, hogy többnyire van beépített tűzfaluk, ami sokkal jobban véd, mint egy Windows-os, szoftveres tűzfal. Továbbá nem emészti a Windows erőforrásait (processzor, memória). Én minden ismerősömnek javaslom egy router beüzemelését, még akkor is, ha csak egyetlen egy számítógépet használ otthon.

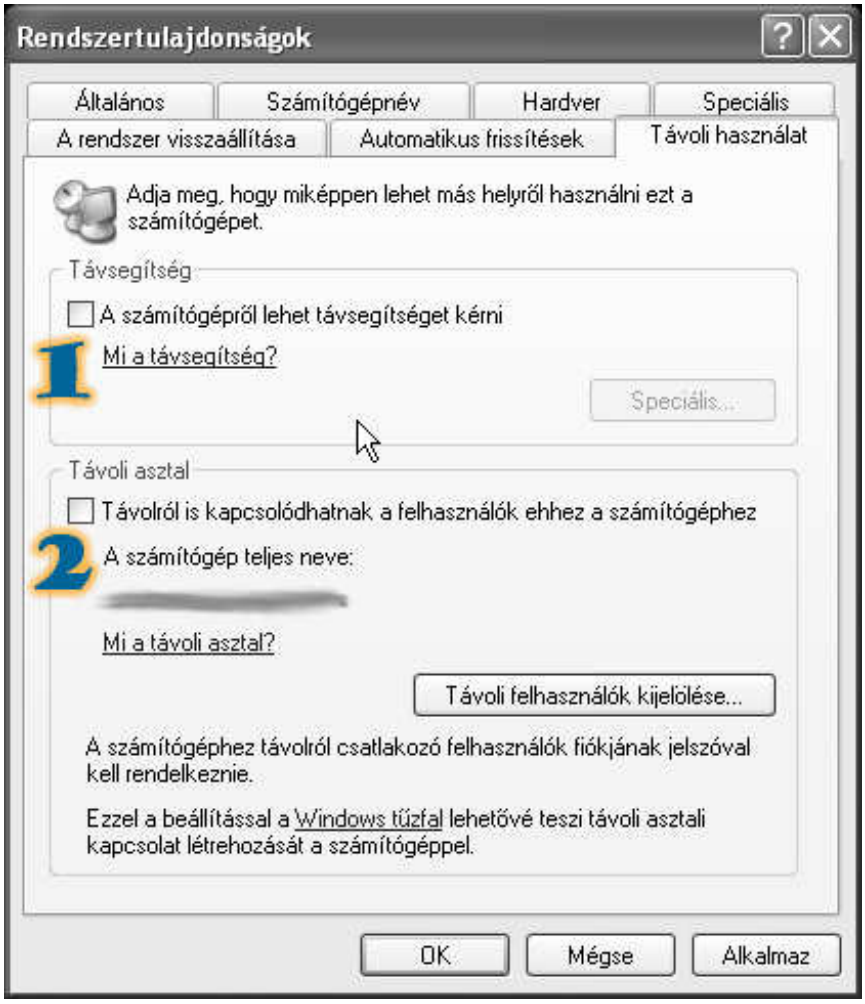
Nem kívánt szolgáltatások letiltása

A Windows XP sok extra szolgáltatást tartalmaz, amit a legtöbb felhasználó nem is használ. Átnézünk néhány olyan szolgáltatást, amit nyugodtan letilthatsz, és ezzel is biztonságosabbá teheted a számítógépedet.

Távoli asztal hozzáférés

A **Távoli Asztal** szolgáltatás lehetővé teszi, hogy hozzáférj a gépedhez távolról, mintha odaülnél a saját billentyűzeted és egered elé, pedig lehetsz akár a világ túlsó végén is. Ez nagyon hasznos lehet egy számítógépes hálózat felügyelete során, de egy otthoni felhasználónak nem biztos, hogy szüksége van rá. A Távoli Asztal nagyon kockázatos alkalmazás, tekintetbe véve, hogy a felhasználók általában nagyon egyszerű jelszavakat használnak. Szóval, ha nem használod távolról a gépedet, akkor az alábbi lépések segítségével javaslom, hogy inkább kapcsold ki ezt a szolgáltatást.

- Kattints jobb egérgombbal a **Sajátgép** ikonon az Asztalon vagy a Start menüben és kérd a **Tulajdonságok**at.
- A **Távoli használat** fül alatt távolítsd el a pipát a **Távsegítség** és a **Távoli asztal** kategóriáknál egyaránt.



3. ábra: A Windows távoli hozzáférésének letiltása

Távsegítség

Ha esetleg technikai segítségre lesz szükséged valakitől az Interneten keresztül, egy nagyon jó lehetőség például az MSN Messenger programon keresztül átadva a géped vezérlését a távoli technikai támogatónak. Ebben az esetben a fenti ábrán látható Távsegítség kategóriában kell a pipa.

Üzenő szolgáltatás

A Microsoft beágyazott az újabb Windows verziókba egy felugró-ablak stílusú üzenetküldő lehetőséget a rendszergazdák számára, hogy könnyebben értesíthessék a helyi hálózat tagjait bármilyen várható eseményről vagy karbantartásról.

Ez egy nagyszerű szolgáltatás – ha jó kezekben van. Sajnos azonban ma már ezt is rossz célokra használják. Akik tudják, hogyan kell használni a szolgáltatást, képesek az Internet hálózatán keresztül felugró-ablak formájában is reklámszemetet terjeszteni, amire kattintva akár kémprogramot is bejuttathatnak a gépedbe. Hogy biztonságban légy erről az oldalról is, **tiltsd le az Üzenetküldő szolgáltatást**!

- Start menü > Futtatás. Utána írd be, hogy **services.msc** és kattints az OK-ra.

- Ekkor betöltődik a szolgáltatás-kezelő. Ebben a listában gördíts lefelé, majd jobb-katt az **Üzenetkezelő**re és válaszd a **Tulajdonságok**at.
- Az **Általános** fülön állítsd az **Indítás típusa** legördülő listát **Letiltva** állapotúra.
- Ha esetleg jelenleg fut, akkor kattints a **Stop** ikonra.
- Végül kattints az OK-ra.

Távoli regisztrációs adatbázis hozzáférés

A regisztrációs adatbázis a Windows legfontosabb része. Itt tárol mindenféle konfigurációs beállítást, és ha nem vigyázol a szerkesztésénél, akkor könnyen használhatatlanná teheted a számítógépedet. Ebből is látható, hogy nagyon kell rá vigyázni.

A Windows XP Professional változatban - az XP Home verzióban nem - van egy olyan szolgáltatás, ami a rendszergazdák dolgát hivatott megkönnyíteni hálózati környezetben azáltal, hogy engedélyezi távolról a regisztrációs adatbázis bejegyzéseinek szerkesztését. Szóval, **ha valakinek van elegendő jogosultsága** (ismeri a rendszergazda jelszót – ha van egyáltalán), **akkor távolról is bármit be tud írni, vagy ki tud törölni a regisztrációs adatbázisból.** Ez túl nagy kockázat ahhoz, hogy így hagyjuk. Az otthoni felhasználók többsége ráadásul soha nem használja ezt a szolgáltatást.

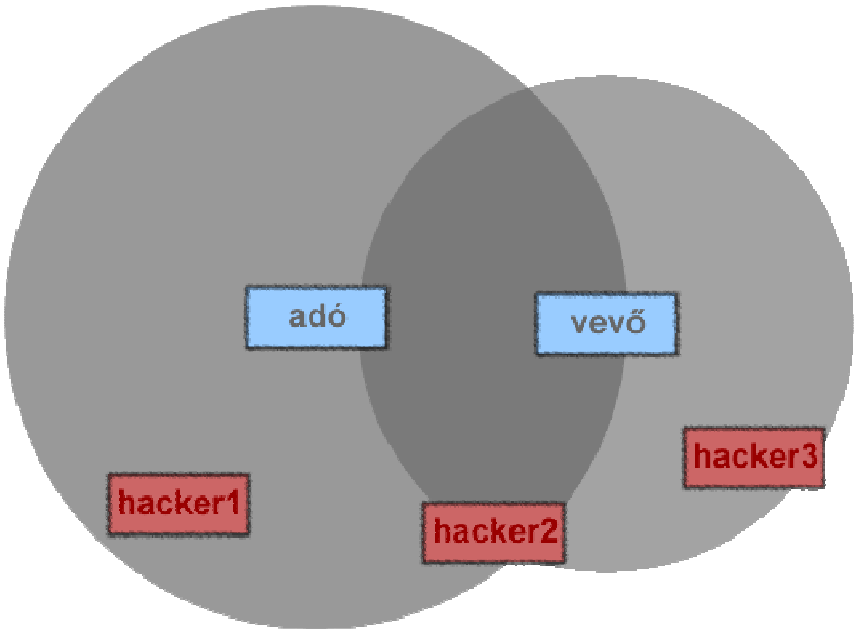
A szolgáltatás letiltásához tedd a következőket:

- Start menü > Futtatás. Utána írd be, hogy **services.msc** és kattints az OK-ra.
- A szolgáltatás-kezelő betöltődésekor gördíts lefelé a listában, majd jobb egérgombbal kattints a **Távoli rendszerleíró adatbázis**ra és válaszd a **Tulajdonságok**at.
- Az **Általános** fülön állítsd az **Indítás típusa** legördülő listát **Letiltva** állapotúra.
- Ha esetleg jelenleg fut, akkor kattints a **Stop** ikonra.
- Végül kattints az OK-ra.

Vezeték nélküli hálózat

A vezeték nélküli hálózatok nagy népszerűségnek örvendenek manapság, mivel kényelmes, mozgatható csatlakozást nyújtanak egy számítógépes hálózathoz. Segítségükkel akár a kertünkben, nyugodt környezetben is leülhetünk dolgozni, vagy csak internetezni egy kicsit. Ez a szabadság könnyen megszokható, de sajnos sokan nem tudják, hogy milyen veszélyeket rejt mindenféle nyílt vezeték nélküli hálózathoz csatlakozni.

Alapvetően a vezeték nélküli kapcsolathoz két eszközre van szükség. Egy adóra és egy vevőre. Nézd meg az alábbi ábrát és utána elmondom, milyen veszélyek vannak, és hogyan védekezhetsz ellene.



4. ábra: Vezeték nélküli hálózat ábrája

Talán leolvasható a rajzról is, hogy az adónak és a vevőnek kölcsönösen egymás hatótávolságán belül kell lenniük. Általában az adó nagyobb teljesítményű, de mindig a kisebb teljesítmény határozza meg a hatótávolságot. Az adó is és a vevő is (hagyományos eszközök esetében) körkörösen sugároz. Ez hozza annak a veszélyét, hogy egy hozzáértő emberke képes „lehallgatni" a rádióátvitelt. **Ha nem használunk titkosítást az adatátvitelhez, akkor akár hangosan is kiabálhatnánk hitelkártya-adatainkat vagy más személyes információnkat.**

Óvakodj a titkosítás nélküli hálózatoktól! Manapság is nagyon sok olyan vezeték nélküli hálózattal találkozom, ahová mindenféle beállítás nélkül beengednek. Az ilyen hálózatokon nem érdemes „érzékeny" adatokkal dolgozni. Maximum szörfözgetni egy kicsit és szórakozni.

A biztonságos hálózatok alapfeltétele valamilyen titkosítás. A legelterjedtebbek a WEP és a WPA titkosítások.

WEP használata

A **WEP (Wired Equivalent Privacy)** volt az első biztonsági szabvány a vezeték nélküli hálózatokhoz. Alapvetően a küldött (oda-vissza) adatokat titkosítja a hozzáférési pont (Access Point) és a kliens között. Kell egy jelszó, melyet titkosítási kulcsként használnak az adatforgalomban.

Ez az egyszerűség egyben a gyengéje is a WEP titkosításnak. A legnagyobb probléma az, hogy az egész rendszer csak egy kulcstól függ. Ha ez a kulcs kitudódik, akkor mindenhol (kiszolgálók, munkaállomások) le kell cserélni a

kódot. Továbbá az is fennállhat, hogy valaki visszafejti a kódot az „elkapott" adatforgalom analizálásával.

Ezen gyengeségek ellenére még mindig jobb, ha WEP-et használunk, mintha titkosítás nélkül kommunikálnánk.

WPA használata

A **WPA (Wi-Fi Protected Access)** egy újabb, továbbfejlesztett biztonsági szabvány a vezeték nélküli hálózatokhoz. Az alapjai ugyanazok, mint a WEP-nek, csak direkt annak gyengeségeit hivatott orvosolni. A WPA-ban már lehetőség van dinamikusan változó kulcsok használatára, sőt, felhasználói név és jelszó kombináció alkalmazására is a hozzáférés szabályozásához.

A WPA használatához (van már WPA2 is) olyan hardver elemek kellenek, amelyek támogatják az adott titkosítást. Érdemes körülnézni a piacon, hogy mind a hozzáférési pont, mind a kliens adaptere támogassa ugyanazt a titkosítást!

A WPA is visszafejthető, csak SOKKAL több ideig tart és SOKKAL nagyobb „elkapott" adatforgalmat kell elemezni. Az már nem biztos, hogy egyszerű szórakozásból valaki nekivág egy akár több napos (kis forgalom esetén akár több hetes, hónapos) folyamatos működésű adatforgalom-naplózásba, csak azért, hogy bejusson a szomszéd lakás hálózatába, ahol lehet, hogy nem is tud majd elérni semmit.

Hozzáférés szabályozása a számítógépedhez

Ha már sikeresen lezártad a számítógéped nyitott portjait és leállítottad a nem használt szolgáltatásokat, akkor itt az ideje, hogy megerősítsd a „főbejáratot", a bejelentkezést. Nem számít, milyen óvintézkedéseket teszel, minden a felhasználói szintű biztonságodra vetül vissza. Ha nincsen jelszavad a saját fiókodhoz és nem vagy védve tűzfallal és egyéb eszközökkel, akkor elég nagy veszélyben vagy támadás szempontjából.

Ezért érdemes odafigyelni a felhasználói fiókokra és azok jogosultságára.

Felhasználói fiókok kezelése

Néhány gyakorlati tanács a felhasználói fiókkezelés beállításaihoz.

Állíts be jelszót és nevezd át a Vendég fiókot
A Windows XP-ben van egy Vendég fiók, ami alapból tiltott. Ez azt jelenti, hogy elvileg Vendég felhasználói névvel hozzá lehetne férni a számítógéphez, csak éppen le van tiltva. Néhány esetben azonban ez a fiók engedélyezetté válhat egy alkalmazás által.

Arra az esetre, ha ez a fiók ismét engedélyezetté válna, javaslom, hogy nevezd át és állíts be hozzá jelszót.

- Start menü > Futtatás. Utána írd be, hogy **lusrmgr.msc** és kattints az OK-ra.

- A Helyi felhasználók és csoportok kezelőjének betöltődésekor jobb egérgombbal kattints a **Felhasználók** kategóriában lévő **Vendég** fiókra és válaszd a **Jelszó megadása…** menüpontot.
- Kapsz egy figyelmeztető ablakot, de csak válaszd a **Folytatást**.
- Mindkét mezőbe írd be ugyanazt a jelszót és kattints az OK-ra.
- Most már csak át kell nevezned. Kattints jobb gombbal a **Vendég** fiókon és válaszd az **Átnevezés** menüpontot.
- Gépelj be egy új nevet (pl.: Tiltott) és **Enter**-rel fejezd be a bevitelt.

Töröld a legutolsó bejelentkező nevét

Ha a klasszikus bejelentkező ablakot használod (be kell írni a felhasználói nevet is és a jelszót is), akkor a bekapcsoláskor a legutolsó belépő nevét már fel is kínálja a rendszer és neked csak a jelszót kell beírni. Ez kényelmes lehet, csak éppen annyira veszélyes is. Ismerni a felhasználó nevét már fél siker a betörés végrehajtásában.

Hogy elrejtsd a legutolsó bejelentkező felhasználó nevét, tedd a következőket:

- Start menü > Futtatás. Utána írd be, hogy **regedit** és kattints az OK-ra.
- Menj el a következő kulcsig: HKEY_LOCAL_MACHINE, SOFTWARE, Microsoft, Windows, CurrentVersion, policies, system.
- Keresd ki a **dontdisplaylastusername** bejegyzést.
- Jobb gombbal kattints rá és válaszd a **Módosítás** menüpontot.
- Gépelj be egy 1-est, kattints az OK-ra és már készen is vagy.
- Ha később mégis szeretnéd visszaállítani, ezt az értéket kell átírnod 0-ra.

Tiltsd le és nevezd át a Rendszergazda fiókot

A Rendszergazda a legfontosabb felhasználói fiók a számítógépen. Nem ajánlatos ezzel a fiókkal használni a számítógépet, mert az biztonsági szempontból nem jó.

Érdemes letiltani és átnevezni a Rendszergazda fiókot, hogy még nehezebbé tedd az ilyen magas jogosultságú hozzáférést a gépedhez:

- Start menü > Futtatás. Utána írd be, hogy **lusrmgr.msc** és kattints az OK-ra.
- A Helyi felhasználók és csoportok kezelőjének betöltődésekor jobb egérgombbal kattints a **Felhasználók** kategóriában lévő **Rendszergazda** fiókra és válaszd a **Tulajdonságok** menüpontot.
- Az **Általános** fülön pipáld be **A fiók le van tiltva** szöveget, majd kattints az OK-ra.

- Kattints jobb gombbal a **Rendszergazda** fiókon és válaszd az **Átnevezés** menüpontot. Adj neki valami más nevet (pl.: Tulaj).

Minden felhasználói fióknak legyen bonyolult jelszava

Ha a géped az Internetre csatlakozik, minden fiókhoz érdemes bonyolult jelszót beállítani. Egy összetett jelszó legalább 7 karakter hosszú és kisbetű, nagybetű, szám, és esetleg különleges karakter is áll benne. Az ilyesmit lehetetlen kitalálni és rengeteg időbe kerülne, amíg próbálgatásos technikával „megfejtenék".

Bonyolult jelszavak kezelése elsőre nem lesz túl könnyű, de a mindennapi használat során hamar megjegyzed majd.

Harc a levélszemét, a kémprogramok és a vírusok ellen

Ez a fejezet megmutatja, hogyan védd meg magad a legnagyobb veszélyektől: levélszemét, kémprogramok, reklámok és vírusok. Mindezek kiirthatók (de legalább is komolyan csökkenthetők) a Windows XP néhány beállításával és különböző védelmi programok használatával.

Vírus (virus)
Számítógépes vírusok már nagyon régóta léteznek. Olyan kis, ártó szándékú programok, amelyek kárt tesznek a számítógép fájljaiban vagy egyszerűen csak lehetetlenné teszik a munkát a géppel.

Levélszemét (spam)
A levélszemét tulajdonképpen azt jelenti, hogy kéretlen levelek kerülnek a postaládádba. Sajnos egyre több és több ilyen e-mail érkezik minden egyes postafiókba. Többnyire hamis gyógyszerek és szexuális teljesítmény-növelők reklámozását találhatjuk meg bennük. Nagyon nehéz megszabadulni tőlük.

Kémprogram (spyware)
A kémprogram egy olyan, titokban telepített segédprogram a gépeden, amely rögzíti a személyes ténykedéseidet vagy egyéb olyan folyamatokat futtat és működtet, amiknek nem örülnél, ha tudnál róla.

Reklám (adware)
A reklámprogram nagyon hasonló a kémprogramhoz, annyi különbséggel, hogy ez még fel is használja a személyes ténykedéseidből nyert információkat, hogy esetleg számodra érdekes reklámokat jelentessen meg, ezáltal nagyon könnyen potenciális vásárlóvá válhatsz, szinte a tudtod és akaratod ellenére.

Kiiktatni a levélszemetet

A spam mindenhol megtalálható manapság. Gyakran tapasztalhatjuk, hogy régóta használt e-mail címünkre elkezdenek érkezni a nem kívánt levelek és rohamosan nő a számuk. Nagyon rövid idő alatt eljuthatunk odáig, hogy már szinte használhatatlan az a címünk, mert nem tudjuk kibogarászni a hasznos leveleket a temérdek szemét közül. Ilyenkor felmerül az emberben, hogy eldobja azt az e-mail címét és inkább másikat használ. Azt hiszem, mindenki tudja az ilyen váltásnak a hátulütőjét. Bizony, mindenkit értesíteni kell az új címről, rengeteg regisztrált helyen meg kell változtatni a címet, és így tovább.

Jó, ha átgondoljuk egész internetes viselkedésünket és már az elején megpróbáljuk kiküszöbölni azt, hogy kikerüljön az e-mail címünk a nem kívánt „köztudatba”.

A Spam megelőzése

Nézzük meg elsőként, hogy miért is kapunk annyi levélszemetet!? A dolog ott kezdődik, hogy a felhasználók mindenféle weboldalon megadják e-mail

címüket, és az oldal tulajdonosa elkezd reklámokat küldeni nekik, vagy eladja az e-mail címeket más cégeknek. Rendszerint a legtöbb honlap figyelmeztet, ha a tervei között szerepel az e-mail címed értékesítése, de ezt általában elrejtik a **Felhasználási feltételek** közé, amit az interneten szörfözők 99%-a nem olvas el, csak bepipálja, hogy elfogadja a feltételeket.

A neten barangolva nagyon oda kell figyelni a részletekre! Ha valamilyen nagyszerű ajánlat miatt feliratkozol egy weboldalon, olvasd el a **Felhasználási feltételeket** (Terms of Services) vagy az **Adatvédelmi nyilatkozatot** (Privacy policy). Ha ilyesmit nem találsz, akkor kezdjen el dolgozni benned a gyanú, hogy nem is olyan megbízható ez a cég és inkább fontold meg, hogy megadod-e nekik az adataidat!

A másik szokásos oka a levélszemét megjelenésének, hogy figyelmetlenül feliratkozunk mindenféle hírlevélre. Általában, ha vásárolunk valamilyen online boltban, ott meg kell adni az e-mail címünket is. Ez eddig rendben is van, de! A rendelés véglegesítésénél többnyire ott van néhány pipálható dolog (nem kifejezetten kiemelve és alapból bepipálva), amelyek azt mondják, hogy kérsz ilyen-olyan hírlevelet is. Ha több online boltban is vásárolgatsz és mindegyiknél feliratkozol 2-3 hírlevélre, akkor igen hamar rengeteg levelet fogsz kapni.

Természetesen a tisztességes szolgáltatóknál lehetőséged van leiratkozni ezekről a hírlevelekről, de mindegyiknél figyelj oda a regisztrációs részletekre! Ha a fenti két tippet hasznosítod, akkor jelentősen lecsökkented a kapott levélszemét mennyiségét.

Több postafiók használatával is sikeresen tudsz harcolni a levélszemét ellen. Nagyon sok ingyenes levelezőrendszer van a neten, ahol regisztrálhatsz különböző e-mail címeket. Készíts néhány címet, melyek mindegyikét más-más célra fogod használni. Nekem is van olyan e-mail címem, amivel regisztrálok olyan oldalakon, ahonnan szeretnék kérni, letölteni valamit, de nem bízom túlságosan a honlap tulajdonosában. Gyakran a letöltéshez küldenek egy megerősítő e-mailt, ezért kell, hogy ténylegesen megkapjam a levelet, de nem zavar, ha az a postafiókom tele van szeméttel. Csak akkor használom, amikor ilyen megerősítéseket küldenek.

Lehet továbbá külön postafiókod csak a család, vagy barátok számára. Ha azt sehol nem publikálod és megkéred barátaidat, hogy ők se adják meg sehol ezt a címedet, akkor biztos, hogy sokáig nem fogsz kapni arra levélszemetet. Idővel persze előfordulhat, hogy valaki ebből a zárt körből pl. vírusos lesz és kikerül a címlistája a spam-küldők kezébe. Ekkor meg fognak jelenni az első levélszemetek a postaládádban.

Szűrő szoftverek használata

Az előző tippek arra szolgáltak, hogy minél kevesebb levélszemetet kapj az idők folyamán. De mi a helyzet, ha már most is nagyon sok szemetet kapsz? Ekkor két lehetőséged van. Vagy e-mail címet váltasz és megpróbálod követni a

fenti tanácsaimat, vagy pedig használsz valamilyen szűrő programot. Az interneten több ezer levélszemét-ellenes (anti-spam) programot találsz. A széles választékban nagyon nehéz megtalálni a nekünk legmegfelelőbb alkalmazást. Nem létezik 100%-os hatékonyságú szűrő, de ami eléri a 90%-ot, az nagyszerű.

A sok közül a spamihilator nevű programot ajánlom. Van hozzá magyar nyelvi csomag is. Ingyenesen letölthető a http://www.spamihilator.com oldalról. Ez a program beépül a levelező programod és a levelező szerver közé és takarítja az ott átmenő leveleket. A finomhangolása megérne egy külön leírást, ezért ebbe a segédletbe nem is illesztem bele. Azonban mindenkit megnyugtatok, hogy alapbeállításokkal is nagyon jól működik.

Külső linkek blokkolása HTML levelekben

Minden alkalommal, amikor levelet kapsz és a levelező programod támogatja a HTML formátumú e-mailek megtekintését, fennáll a lehetősége, hogy a küldő nyomon kövesse, vajon elolvastad-e a levelét vagy sem. Ezt úgy oldják meg, hogy egy nem látható képet is beillesztenek a levélbe, és amikor azt megpróbálja betölteni a levelező program, akkor valójában egy visszajelzést ad a küldőnek, hogy ez az e-mail cím él és használatban van – tehát lehet további szeméttel tömni, mert a tulajdonos elolvassa a leveleket.

A spammelők ezt a technikát is használják arra, hogy kitakarítsák az adatbázisukból a nem létező, vagy nem használatos e-mail címeket. Ha tehát nem jeleníted meg a képeket, idővel törölhetnek az adatbázisukból és nem kapsz több levélszemetet tőlük.

Szerencsére az Outlook 2003 már automatikusan blokkolja a külső hivatkozásokat a HTML üzenetekben. Továbbá az Outlook Express is ezt teszi a Windows XP Service Pack 2 óta. **Mindenképpen érdemes** tehát **frissíteni a rendszeredet** és legalább az SP2-t fel kell telepíteni, ha Windows XP-t használsz!

Védekezés a kém- és reklámprogramok ellen

Az elmúlt években a kémprogramok lettek a legnagyobb veszélyforrások a számítógépekre. Általában ingyenes programokba rejtve, ezek az alkalmazások kikémlelik a számítógépeden történteket és jelentik a szokásaidat az üzemeltetőiknek. A reklámprogramok hasonlóan viselkednek, csak éppen elemezve a szokásaidat, ha eljön a megfelelő pillanat (éppen keresel valamit a neten), bekínálnak neked egy reklámot, ami kötődik az érdeklődési körödhöz.

Hogyan fertőződsz meg az ilyen programokkal? Sok lehetőség van, de a leggyakoribb az, hogy meglátogatsz egy weboldalt, ami arra kér, hogy kattints az Igen-re egy telepítési kérdésnél, és Te azt hiszed, most telepítesz egy kis játékprogramot, amit ki akarsz próbálni. Lehet, hogy játékot IS telepítesz, de fennáll a veszélye annak, hogy éppen most fertőzted meg a számítógépedet.

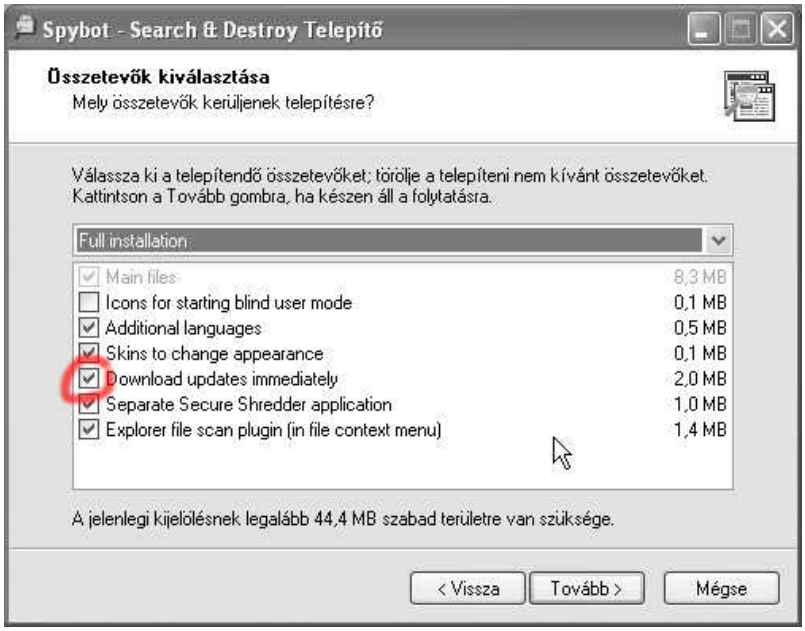
Sajnos a felhasználók szinte soha nem olvassák el a felhasználási feltételeket, amikor ingyenes segédprogramokat telepítenek a gépükre. Pedig ott általában le van írva, hogy ezzel a programmal együtt feltelepíted az XY cég ilyen-olyan adware programját is. Az alábbiakban néhány hasznos tanácsot olvashatsz ezek kivédése érdekében.

Felderíteni és eltávolítani a kémprogramokat

Rengeteg ingyenes segédprogram van ebben a témakörben is az interneten. Vigyázni kell, mert újabban azt a trükköt is alkalmazzák, hogy kémprogram-eltávolítónak hirdetik a programot, miközben ő maga a kémprogram. Érdemes utánanézni (Google) a kiválasztott programnak, mit is ír róla valójában a netes társadalom.

Én személy szerint az ingyenes Spybot S&D (Search and Destroy) programot javaslom, ami nagyon jól viselkedik. A programot töltsd le és telepítsd a következő címről: http://www.spybot.info.

A telepítés során felmerülhet néhány kérdés. Ezeket külön elmagyarázom, amit pedig nem emelek ki, annál egyszerűen a Tovább gombot kell nyomni.



5. ábra: Spybot telepítés, frissítéssel együtt

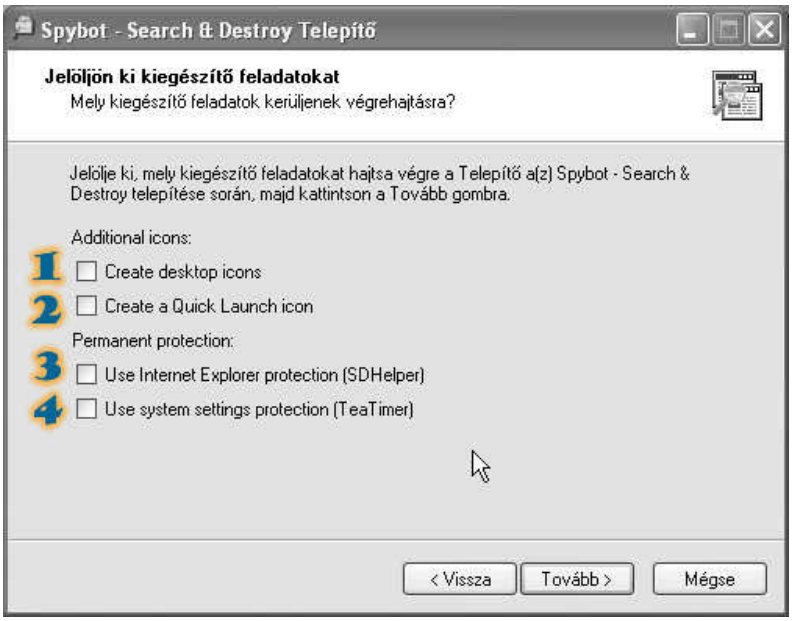
Az 5. ábrán látható képen megjelölt pipát érdemes kiszedni akkor, ha a gép nem csatlakozik az internetre, különben nem fog végigmenni a telepítés.

A 6. ábrán (lsd. alább) lévő felsorolás magyarázata a következő:

1. Készítsen parancsikont az asztalra
2. Készítsen parancsikont a gyorsindítás eszköztárra (a Start menü mellett)
3. Megvédi az Internet Explorert. Védi az IE beállításait, mint pl.: kereső- és kezdőlap módosítása, eszköztárak telepítése, stb.

4. Megvéd néhány rendszerbeállítást, mint pl.: ha a gép bekapcsolásakor egy program beállítja magát automatikus indításra

Tapasztalataim szerint egy egyszerű, halandó felhasználónál inkább csak problémát okoz, ha a Spybot minden felmerülő védelmi kérdésnél feldob egy kérdező ablakot, ezért inkább javaslom a 3. és 4. pontnál lévő pipák kiszedését.



6. ábra: Spybot telepítési beállítások

7. ábra: A Spybot S&D nyitóképernyője

Első indításkor érdemes kiválasztani a kívánt nyelvet (Language). A sikeres használathoz mindenképpen szükséges legalább hetente frissíteni (**Search for Updates**) a program adatbázisát (lsd. 7. ábra). Ha megtörtént a frissítés, akkor már csak a **Mind keresése** gombra kell kattintani és várni. A keresési folyamat függ a számítógép hardverétől, de akár 20-50 perc is lehet.

Ha befejezte a keresést (lsd. 8. ábra), akkor megjelenik egy találati lista és egy újabb nyomógomb. Alapesetben minden találat be van pipálva, így aztán csak a

Kijelöltek javítása feliratú gombra kell kattintani és készen is vagyunk a takarítással.

Immunizáld a rendszeredet! A Spybot sokkal többre képes, mint csak felkutatni és eltávolítani a számítógépeden lévő kártevőket. Ezeken felül felkínálja az immunizálás lehetőségét néhány közismert kémprogram ellen, ami azt jelenti, hogy a számítógéped védett lesz azokkal a károkozókkal szemben.

Az immunizálás bekapcsolásához tedd a következőket:

- Indítsd el a Spybot S&D programot.
- Ha elindult, a bal oldali gombok közül nyomd meg először a **Frissítés**t és csináld végig a letöltés folyamatát.
- Ha készen van a Frissítés, kattints az **Immunizálás** gombra.
- Az itt megjelenő menügombok közül kattints az elsőre (**Immunizálás**).

Ezeket a lépéseket **ismételd meg legalább kéthetente** és utána futtass végig egy teljes **Keresés és megsemmisítés**t is!

Védelem a vírusokkal szemben

A Windows XP-nek az SP2 óta sok olyan új tulajdonsága van, amelyek az eddigi legbiztonságosabb Microsoft operációs rendszerré tették. Az egyik ilyen a futtatás-védelem, mely az új processzorok hardveres védelmét használja ki.

Az egyik leggyakoribb típusa a számítógépes betöréseknek és vírusfertőzéseknek a „buffer túlcsordulás". Ez akkor fordul elő, amikor adatokat küldünk buffernek, gyorsabban, mint ahogy a processzor fel tudja dolgozni azt. Amikor a buffer megtelik, a rendszer bizonytalanná válhat, és néha lefuttatja azt a kódot, amit a bufferbe helyeztek. Így terjed nagyon sok vírus. Kihasználják az ellenőrizetlen bufferek előnyeit és lefuttatják az ártó kódjaikat. Az egyik a könnyű megoldás erre, hogy a processzorba építenek egy olyan védelmet, ami nem engede semmilyen buffer adatát futtatni. Ezzel a vírus ugyan be tudja tölteni magát a bufferekbe, de soha nem lesz képes onnan lefutni, azaz továbbterjedni.

buffer

A buffer egy átmeneti tároló, amellyel a számítógép megpróbálja gyorsítani a működését. Sok területen használják a gépben. Talán egy példán keresztül jobban megérthető, mire is szolgálnak a buffer-ek. Aki régebbi gépekkel is dolgozott, biztosan találkozott azzal, hogy egy szövegszerkesztőben gépeli a szöveget, a Windows csak homokórázik és egy kis késleltetéssel jelennek meg egyszerre a beírt karakterek, amikor a processzor ráér foglalkozni a beviteli eszközzel. Bizony, a billentyűzet olvasásához is buffert használ a számítógép.

Ez a védelem az AMD Athlon 64, és az Intel Pentium 4 Prescott processzoroktól kezdve található meg a gépekben. Ha ilyen, vagy újabb processzorod van a gépben, akkor a Windows engedélyezi ezt a védelmet. Mindazonáltal néhány programnál hibás működést eredményez ez a védelem,

mert azokat úgy programozták, hogy kihasználják a buffer túlcsordulás lehetőségét, és ha ez le van tiltva, akkor nem működik helyesen. Erre építettek be a Windows-ba egy kivétel listát. Arra azonban mindig figyelj oda, hogy tényleg **csak olyan program szerepeljen a kivételek között**, aminek a működésével egyébként gondjaid vannak! Ha szerkeszteni akarod a listát, tedd a következőket:

- Kattints jobb egérgombbal a **Sajátgép** ikonon az Asztalon vagy a Start menüben és kérd a **Tulajdonságok**at.
- Ha betöltődött a **Rendszertulajdonságok** ablak, kattints a **Speciális** fülre.
- Ott kattints a **Teljesítmény** szakasz **Beállítások** gombjára.
- Vedd elő az **Adatvégrehajtás megakadályozása** fület és a választógomb az alsónál legyen (Adatvégrehajtás megakadályozása az összes programnál és szolgáltatásnál, kivéve:)
- Nézd át az ott lévő listát (ha van ott valami) és tényleg csak azt hagyd benne, ami egyébként nem működik helyesen. Minden mást jelölj ki és távolíts el!
- Kattints az OK-ra és még egyszer kattints az OK-ra, hogy bezárd a Rendszertulajdonságok panelt is.

Használj vírusirtó programot

Ha nem használsz vírusirtó programot és kapcsolatban vagy az Internettel, akkor azonnal kapcsold ki a számítógépedet! Erősen ajánlom, hogy csak vírusvédelemmel ellátott számítógépet csatlakoztass a világhálóra! A vírusvédelem akkor jó, ha az adatbázisa nem régebbi egy hétnél, azaz naprakész. Egyéb esetben teljesen felesleges vírusirtót használnod, ha nem frissíted rendszeresen.

Ha nem akarsz több ezer forintot költeni évente egy vírusirtó programra, nagyon sok ingyenes megoldás is létezik. Én személy szerint a Grisoft cég AVG programját szoktam ajánlani ismerőseimnek.

AVG free edition
Az AVG ingyenes vírusirtójához a következő helyről tudsz hozzájutni: http://free.avg.com. A Grisoft cégnek van komplett internet-biztonsági csomagja is, de az nem ingyenes. Figyeljünk oda tehát, hogy az ingyenes (free) változatot töltsük le és később se engedjünk a szoftver kérésének, hogy próbáljuk ki a teljes körű védelmet nyújtó egyéb programjait. Igaz, hogy ez „csak” vírusvédelem, de legalább ingyenes. Kémprogram-védelemről pedig már szintén ejtettem néhány szót egy korábbi fejezetben.

Védd meg a magánéletedet

A Windows XP nyomon követi a tevékenységedet, amit számítógépeden végzel. Eltárolja a látogatott weboldalakat, a begépelt címeket, a futtatott programokat és még a megnyitott fájlok listáját is. Miért is teszi ezt? Elsődlegesen a Te kényelmed érdekében naplózza ezeket a dolgokat, hiszen így tud neked segíteni a legutóbbi dokumentumok vagy a legutóbb használt programok listájával. A meglátogatott weboldalak címének eltárolása is a Te kényelmedet szolgálja.

Mindenesetre ezek az információk rossz kezekbe kerülve másra is felhasználhatók. A magánéleted is nyílt titokká válhat, ha mások hozzáférnek a számítógépedhez. Ez a fejezet megmutatja, hogyan távolítsd el a kényes információkat a gépedről.

Internet Explorer

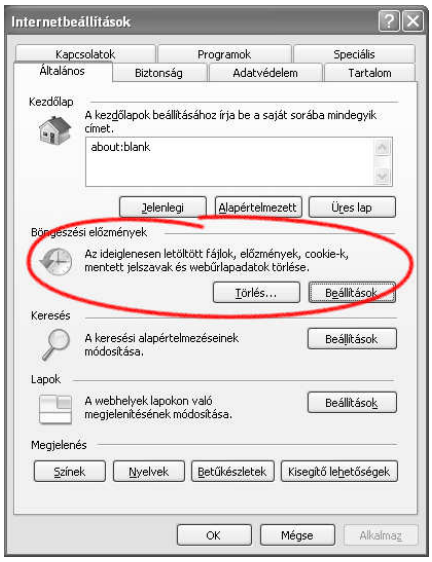
Az Internet Explorer takarítása a Windows egyik legbonyolultabb része, mivel mindenfelé tárolja az adatait. Főként a következő részeket kell takarítani: legutóbbi címek, előzmény fájlok, átmeneti webfájlok és cookiek.

Címsor kiegészítés eltávolítása

Az össze Windows verzióban az automatikus kiegészítés aktiválva van a böngésző címsorára (ahová beírod a weboldal címét). Ez azt jelenti, hogy amikor elkezded begépelni azt, hogy **www.o**, akkor a korábban begépelt, o-val kezdődő (pl.: origo.hu) oldalt fel fogja kínálni neked és már nem is kell tovább gépelned.

Hogyan állíthatod le ezt a szolgáltatást? Az Internet Explorer 7-es verziójában menj az Eszközök > Internetbeállítások menüpontra. A megjelenő párbeszédpanel közepe tájékán találod az előzményekre vonatkozó beállításokat (lsd. 8. ábra). Választhatsz, hogy most csak törölni akarod az előzményeket, vagy módosítod a beállításokat is (pl.: csak egy napig tárolja).

Nézzük meg tüzetesebben, miket lehet törölni az előzmények közül. Ehhez nyújt segítséget a 9. ábra.



8. ábra Internetbeállítások párbeszédpanel

9. ábra Böngészési előzmények törlése

Látogatott oldalak listájának törlése

Alapesetben az IE 7-es verziója 20 napig őrzi meg a látogatott oldalak listáját. Ezt a beállításoknál (lsd. 8. ábra > Beállítások) át lehet írni akár 0 napra is. Ha kényes vagy a magánéletedre, akkor érdemes gyakran ürítened az előzmények listáját (lsd. 9. ábra > Előzmények törlése).

Ha ezt teszed, akkor bárki használja is a gépedet, megnehezíted a dolgát, hogy kitalálja, mit csináltál a neten. Azért tartsd fejben, hogy ha kitörlöd az előzményeket, akkor esetleg nem tudsz majd visszalépni egy korábban látogatott oldalra, ha elfelejted az URL-jét.

Átmeneti internet-fájlok és sütik törlése

Minden alkalommal, amikor meglátogatsz egy weboldalt, az oldal tartalma (képek, video, szöveg, stb.) letöltődik és egy átmeneti tárolóba kerül. Ezt a könyvtárt hívják Temporary Internet Files (Ideiglenes Internet Fájlok) mappának. Idővel ez a mappa megtelik azon honlapok tartalmával, amiket meglátogattál és elég sok helyet is képes lefoglalni a merevlemezen. Ha egy másik felhasználó odaül a gépedhez, és átnézi ezt a könyvtárat, ki tudja találni belőle, hogy merre szörfözgettél.

A sütik (cookies) olyan átmeneti elemek, amik honlapok látogatásakor jönnek létre a gépeden. Valójában a sütik nem annyira ártó dolgok, mert nagyon sok honlap kényelmi szolgáltatásainak használatához szükségesek. Az egyik ilyen például az automatikus beléptetés egy honlapra. Hirdetők is gyakran használják személyes adatok tárolására, például, hogy ne mutassa az adott oldal 50-szer ugyanazt a reklámot neked.

Tévhit, hogy a sütik adatokat küldözgetnek egyik weboldalról a másikra. A sütik akkor lehetnek veszélyesek, ha egy másik felhasználó hozzáfér a számítógépedhez és átnézi a süti-listádat. Ott ugyanis láthatja, hogy milyen oldalakat látogattál és azt is, hogy milyen felhasználói névvel vagy ott regisztrálva, stb.

A fenti két kategória törléséhez kattints a törlésre az Ideiglenes internetfájlok és a Cookie-k után (lsd.: 9. ábra).

Ezzel megnehezíted az utánad kíváncsiskodók dolgát és még egy kis helyet is szabadítasz fel a merevlemezen.

Süti-biztonsági szabályok beállítása

Mint az előbb is említettem, a sütik nem annyira rosszak, mint ahogy mondják róluk. Valójában az egyetlen igazi veszélye, hogy veszíthetsz egy kicsit a magánéletedből. Ha engedélyezed a böngésződnek, hogy elfogadja a sütiket, akkor idővel szép kis kollekciód jöhet össze, amiből egy hozzáértő és a számítógépedhez hozzáférő emberke kielemezheti bizonyos szokásaidat.

Az Internet Explorer legutóbbi verziója sok fejlesztést tartalmaz. Már választhatsz, hogy milyen sütiket fogadsz el. Ehhez azonban nézzük meg a sütik lehetséges fajtáit. Van first-party (belső) és third-party (külső) süti. A böngésző elnevezéseit követve írtam belső és küldő sütit, mert abban így fogod megtalálni. A belső süti közvetlenül az általad meglátogatott weboldaltól származik és ő helyezi le a te számítógépeden. A külső sütit egy másik számítógép (harmadik fél) helyezi (helyezné) el a gépeden, mint például a reklám-kiszolgáló.

Ha nem akarod kapásból elfogadni az összes sütit, akkor tedd a következőket:

- Indítsd el az Internet Explorert.
- Válaszd az **Eszközök** menü **Internetbeállítások** menüpontját.

- Válaszd ki az **Adatvédelem** lapfület. Itt látsz egy csúszkát, de javaslom, hogy azt hagyd békén és inkább kattints a **Speciális gomb**ra.
- A megjelenő párbeszédpanelen pipáld be „Az automatikus cookie-kezelés felülbírálata” jelölő négyzetet
- Most már tudod állítani a süti-kezelést. Javaslom, hogy mindig fogadd el a belső sütiket és döntsd el, hogy elutasítod vagy rákérdezzen a külső sütikre. Utóbbi esetben kapsz egy kérdező párbeszédpanelt, ahányszor csak egy külső süti próbálna meg ráülni a gépedre.
- A Munkamenet sütiket mindig fogadd el!
- OK és ismét OK a párbeszédpanelek bezárásához

10. ábra Sütikezelés beállítása

Ezek után persze érdemes törölnöd az eddigi sütijeidet. Ezt a 9. ábrán látható Cookie-k törlése gomb megnyomásával teheted meg.

Titkosított oldalak mentésének tiltása

Ha a banki ügyeidet vagy vásárlásaidat interneten keresztül rendezed, bizonyára találkoztál már a biztonságos internet-kapcsolat fogalmával vagy más néven az SSL-el. Ez általában a címsorban úgy jelenik meg, hogy az URL https:// -el kezdődik. Ilyenkor egy biztonságosan kódolt kommunikáció zajlik a géped és a szerver között. A Te gépeden viszont a megjelenítés miatt ki kell kódolni a fájlt és ezt is elmenti a Temporary Internet Files mappába.

Ez alapból eléggé kockázatos, mert ha valaki hozzáfér a gépedhez (vagy csak távolról a fájljaidhoz), fel tudja deríteni az ilyen biztonságos odalaknak egy pillanatnyi tükörképét, például hozzáférhet a banki információidhoz (számlaszám, hitelkártyaszám, átutalások, egyenleg, stb.). Mindehhez nem kell tudnia a jelszavadat sem.

Mit tehetsz ezek kivédése érdekében? Van egy jó kis szolgáltatás az Internet Explorerben, amit csak be kell kapcsolnod és máris megszüntetted a problémát. Kövesd a következő lépéseket:

- Indítsd el az Internet Explorert.

- Válaszd az **Eszközök** menü **Internetbeállítások** menüpontját.
- Menj át a **Speciális** lapfülre. Itt a Biztonság kategórián belül gördíts le a „**Titkosított lapokat ne mentsen a lemezre**" szövegig és pipáld be.
- Kattints az OK-ra és készen is vagy.

Automatikus kitöltés letiltása

Már meséltem az automatikus kitöltésről a címsorral kapcsolatban. A Windows azonban nem csak ahhoz használja az automatikus kitöltést. Egy másik hely, például a weboldalakon lévő űrlapok kitöltése. Ha egy bizonyos nevű mezőbe elkezdesz gépelni valamit (mondjuk felhasználói név), és már jártál azon az oldalon, akkor fel fogja kínálni a hasonló betűvel kezdődő, korábban már begépelt variációkat.

Ez a képesség lehetővé teszi bárki számára (aki hozzáfér a gépedhez), hogy lássa például, hogy milyen kereséseket végeztél korábban, vagy milyen felhasználói névvel lépsz be egy adott honlapon. Még akkor is, ha a böngésző előzményeit törölted.

Ezt a képességet egyébként a böngésző a legelső használatkor állítja be és megkérdezi, hogy akarod-e az automatikus kiegészítést. Én ilyenkor szoktam neki mondani, hogy nem és már készen is vagyok. Ha nálad működik ez a szolgáltatás, és szeretnéd kikapcsolni, akkor tedd a következőket:

- Indítsd el az Internet Explorert.
- Válaszd az **Eszközök** menü **Internetbeállítások** menüpontját.
- Menj át a **Tartalom** lapfülre. Ott az Automatikus kiegészítés kategóriánál kattints a **Beállítások** gombra.
- Szedd ki a pipát mindegyik jelölőnégyzetből.
- Kattints az OK-ra majd ismét az OK-ra.

Ideiglenes Internet Fájlok automatikus törlése

Korábban elmondtam, hogyan tudod törölni az ideiglenes internet fájlokat. A használat során azonban nagyon hamar újra felhalmozódnak a látogatott weboldalak fájljai, amelyek ismét biztonsági kockázatot jelentenek. Erre van egy egyszerű megoldás.

Az Internet Explorerben kell beállítani, hogy kilépéskor takarítsa ki az ideiglenes internet fájlok tárolására szolgáló mappát. Ennek beállításához tedd a következőket:

- Indítsd el az Internet Explorert.
- Válaszd az **Eszközök** menü **Internetbeállítások** menüpontját.
- Menj át a **Speciális** lapfülre. Itt a Biztonság kategórián belül gördíts le „**Az ideiglenes internetfájlok törlése a böngésző bezárásakor**" szövegig és pipáld be.

- Kattints az OK-ra és készen is vagy.

Ha engedélyezed az automatikus törlést, az egy nagyszerű módja a számítógéped tisztántartásának. Ez a sütiket nem fogja törölni, csak a látogatott weboldalak tartalmát a helyi gépeden.

Windows felület

Ha már végre kordában tartod az Internet Explorert, áttérhetünk a Windows felület többi részére. Az Internet Explorerhez hasonlóan a Windows Intéző is sok információt tárol a géphasználatoddal kapcsolatban. Ilyen a legutóbbi dokumentumok listája és a leggyakrabban használt programok listája is. Ezek elvileg a számítógéped mindennapi használatának meggyorsítását szolgálják, de akár nem kívánt információkat is szolgáltathatnak rólad mások számára.

Gyakran használt program-lista ürítése

Az egyik nagyszerű szolgáltatása a Windows XP-nek akár fájó ponttá is válhat, ha kényes vagy a magánéletedre. A gyakran használt programok könnyű elindítása (nem kell végignavigálni a Start menün) időt takarít meg számodra. Azonban e miatt bárki, aki hozzáfér a gépedhez, láthatja, milyen programokat használsz gyakran.

Ennek kivédésére az egyik megoldás, hogy a Start menüt átállítod klasszikus stílusra. Ebben a felállásban nincs helye a gyakran használt programoknak. Ha ezt szeretnéd, kövesd az alábbiakat:

- Kattints a **Start** gombra jobb egérgombbal és válaszd a **Tulajdonságok** menüpontot.
- A választókapcsoló legyen a „**Klasszikus Start menü**” bejegyzésen.
- Kattints az OK-ra és készen is vagy.

Ha azonban szereted az újabb Windows XP menüt és továbbra is azt akarod használni, akkor a gyakran használt programok listájának törléséhez a következőket kell tenned:

- Kattints a **Start** gombra jobb egérgombbal és válaszd a **Tulajdonságok** menüpontot.
- A választókapcsoló legyen a „**Start menü**” bejegyzésen és kattints mellette a **Testreszabás** gombra.
- Az **Általános** lapfülön a **Lista törlése** gombra kattintva tudod kiüríteni a gyakran használt programok listáját. Ezek után majd újra elkezdi felépíteni ezt a listát a Windows a használat függvényében.
- A törlés gomb mellett láthatod, hogy alap esetben maximum a 6 leggyakoribb programot jeleníti meg a Windows. Ha ezt átállítod 0-ra akkor is kilőtted ezt a szolgáltatást.
- Kattints az OK-ra és készen is vagy.

Nem kell megijedni! Ez nem törli a programot, csak a gyors elérésből veszi ki. A Start menün, vagy az asztali parancsikonon keresztül továbbra is indíthatóak a programok.

Legutóbbi dokumentumok listájának törlése

A Windows XP a legutóbb megnyitott dokumentumaidat is kigyűjti egy gyorslistába, melyen keresztül könnyen megnyithatod őket. Ebben a listában (az előzőhöz hasonlóan) szintén csak parancsikonok vannak, tehát a dokumentum nem törlődik, ha kiüríted a listát. Megnehezíted viszont azok dolgát, akik szeretnének rábukkanni a gépeden az esetleg kényes dokumentumaidra. Én valójában nagyon ritkán használom ezt a szolgáltatását a Windows XP-nek.

A lista törlése ismét két verzióra bomlik. Ha a Klasszikus Start menüt használod (lsd. feljebb), akkor kövesd az alábbi lépéseket:

- Kattints a **Start** gombra jobb egérgombbal és válaszd a **Tulajdonságok** menüpontot.
- A választókapcsoló legyen a „**Klasszikus Start menü**” bejegyzésen és kattints a **Testreszabás** gombra.
- A megjelenő párbeszédpanelen kattints a **Törlés** gombra.
- Kattints az OK-ra és készen is vagy.

Ha az újabb Start menü elrendezést használod, akkor a következőket kell tenned a legutóbbi dokumentumok listájának törléséhez:

- Kattints a **Start** gombra jobb egérgombbal és válaszd a **Tulajdonságok** menüpontot.
- A választókapcsoló legyen a „**Start menü**” bejegyzésen és kattints a **Testreszabás** gombra.
- A megjelenő párbeszédpanelen válaszd a **Speciális** lapfület.
- Az ablak alján kattints a **Lista törlése** gombra.
- Ha a későbbiekben sem szeretnél listát, vedd ki a pipát „**A legutóbb megnyitott dokumentumok listázása**” elől.
- Kattints az OK-ra, majd még egyszer és készen is vagy.

Átmeneti fájlok törlése a merevlemezről

Idővel a merevlemezed telítetté válhat azokkal az átmeneti fájlokkal, amelyeket különböző alkalmazások és az operációs rendszer hagy maga után. Ezek nem csak a helyet foglalják, hanem akár információkkal is szolgálhatnak a számítógéped használatáról. Érdemes néha üríteni az átmeneti fájlok tárolására használt mappát.

A régebbi Windows-oknál egyszerűbb volt a dolog, mert csak egy Temp könyvtár volt, amit erre a célra használt. A Windows XP azonban már több

ilyen mappát is tartalmaz, attól függően, hány önálló felhasználó van az adott számítógépen. A következő mappák tartalmát kell kiüríteni:

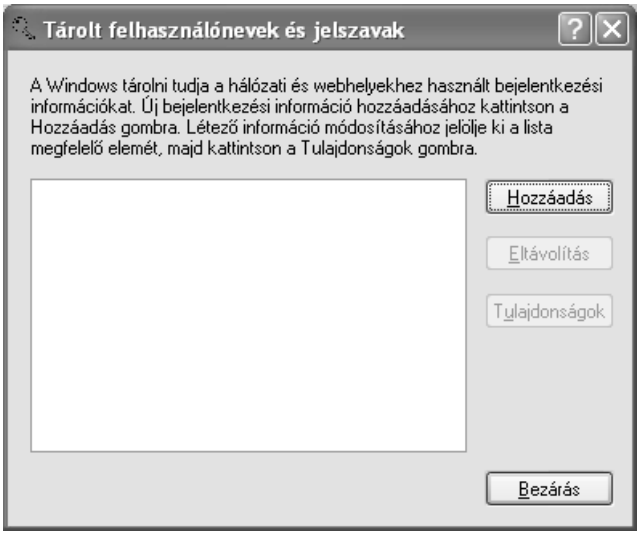
- C:\WINDOWS\Temp
- C:\Documents and Settings**Felhasználó**\Temp
- C:\Documents and Settings**Felhasználó**\Local Settings\Temp

Természetesen, ha a Windows másik meghajtóra és/vagy könyvtárba van telepítve, akkor az útvonalak változhatnak és a **Felhasználó** helyett mindenkinek be kell helyettesítenie a saját felhasználói nevét. Azt azért már hadd ne mondjam el, hogyan kell fájlokat törölni a Windows XP rendszerben! Legyen elég annyi, hogy megoldható a Sajátgép ikonon keresztül is.

Elmentett jelszavak törlése

Amikor meglátogatsz egy weboldalt, ami hitelesítést igényel, vagy csatlakozol egy távoli számítógéphez, mindig megvan a lehetőséged, hogy elmentsd a jelszavadat és legközelebb nem kell begépelned azt, ha újra használni akarod azt a szolgáltatást. Ennek sok kényelmi előnye van, de félelmetes veszélyei is. Ha valaki odaül a gépedhez, akár úgy tudja használni bizonyos fiókjaidat (e-mail, banki oldalak, közösségi oldalak, webboltok, stb.), mintha Te magad ülnél ott. Ez azért szerintem egy kicsit felelőtlen!

Másik veszélye, hogy mivel nem használod rendszeresen a jelszavadat (hiszen úgyis el van mentve), nem fogsz emlékezni rá, amikor egy másik számítógépről kellene használnod a szolgáltatást, vagy mondjuk újra kellett telepíteni a gépedet. Ezért is mindenképpen azt javaslom, hogy **soha ne tároljuk el a jelszavakat**, inkább használjuk a saját szürkeállományunkat (gy.k. az agyunkat) rendszeresen. Ez az elején macerásabb, de idővel belerázódunk és egy kicsit a memóriánkat is karbantartjuk vele.



11. ábra Tárolt felhasználónevek és jelszavak

Ha kíváncsiak vagyunk, hogy milyen szolgáltatásokhoz tartozó jelszavak vannak eltárolva a rendszerünkben, kövessük az alábbi útmutatót.

- Kattints a Start menü > Futtatás parancsra.
- Írd be, hogy **rundll32.exe keymgr.dll,KRShowKeyMgr**
- Megjelenik az eltárolt felhasználói nevek és jelszavak listája.
- Ha valamelyiket szeretnéd kitörölni, jelöld ki és kattints az **Eltávolítás** gombra. A törlési kérést meg kell erősítened.
- Ha befejezted a törölgetést, csak kattints a **Bezárás** gombra.

Fájl- és mappajogosultságok beállítása

Ha a Windows XP operációs rendszert az NTFS fájlrendszerrel használod, akkor lehetőséged van egyenként felhasználói jogosultságot állítani fájlokhoz és mappákhoz egyaránt. Fájl és mappa jogosultságok beállításával szabályozhatod, hogy ki képes olvasni, írni, futtatni, kilistázni vagy hozzáférni egy mappa tartalmához vagy egy fájlhoz. Így aztán a jogosultság beállítása igen hatékony eszköz az adataid megvédésére.

Jogosultságok beállításához először is le kell tiltanod az alapértelmezett egyszerű fájlmegosztást. Ehhez tedd a következőket:

- Nyiss meg bármilyen mappát a gépeden (pl.: Dokumentumok).
- Válaszd az **Eszközök** menü **Mappa beállításai** menüpontját.
- Menj a **Nézet lapfül**re és gördíts lefelé addig, míg meg nem látod az „**Egyszerű fájlmegosztás használata (ajánlott)**” szöveget.
- Távolítsd el a pipát előle.
- Kattints az OK-ra és máris visszanyerted a teljes szabályozást a fájlrendszered felett.

Most már hozzá fogsz férni a mappák és fájlok jogainak beállításához. Ez egyébként nagyon egyszerű folyamat, amire néhány használat után magad is rá fogsz jönni. A jogosultság beállításához tedd a következőket:

- **Jobb egérgombbal** kattints bármelyik mappára vagy fájlra, aminek módosítani szeretnéd a jogait és válaszd a **Tulajdonságok** menüpontot.
- A megjelenő párbeszédpanelen válaszd a **Biztonság lapfül**et. (Amíg az egyszerű fájlmegosztás engedélyezve volt, addig ez a fül nem látszott.)
- Elsőként távolítsd el az összes bejegyzést a **Csoport vagy felhasználó neve** ablakból, akiknek nem akarsz hozzáférést adni az adott objektumra. Jó ötlet eltávolítani a Mindenki nevű csoportot, hiszen a neve is mutatja, hogy mindenki beletartozik. **Arra azért figyelj oda, nehogy véletlenül a saját felhasználói nevedet is kitöröld és lehetőleg a SYSTEM csoportot se bántsd!**

Ha örökli az engedélyeket…
Ha nem sikerül eltávolítani felhasználókat a csoportból, az azért lehet, mert az objektum a szülő könyvtártól örökli az engedélyeket. Az engedélyek minden almappára hatással vannak. Ha mégis csak egy adott mappához szeretnél engedélyt

állítani neki, de az almappáihoz nem, akkor alul a **Speciális** gombra kell kattintanod. A megjelenő párbeszédpanelen vedd ki a pipát „Az örökölt engedélyek alkalmazása" elől. Ekkor egy biztonsági figyelmeztetés jelenik meg, amelynél nyugodtan kattinthatsz az Eltávolítás gombra, és ezáltal minden örökölt engedély ki fog törlődni és szabadon állítgathatod a mappa jogosultságát.

- Most már egyenként választhatod, hogy a fenti ablakban kijelölt felhasználóhoz az alsó ablakban milyen engedélyeket adsz meg.
- Ha készen vagy a beállításokkal, kattints az OK-ra.

Tartsd fejben, hogy az engedélyek alap esetben öröklődnek az almappákra és tartalmukra! Továbbá nem javasolt a gyökérkönyvtár és rendszermappák jogosultságainak állítgatása.

Összefoglalás

Köszönöm kitartó figyelmedet!

Mostanra remélem egy kicsit jobban megismerted a Windows rendszeredet és más szemmel tekintesz rá. Nem árt, ha tudjuk, mivel dolgozunk vagy szórakozunk! Ha a könyvben említett tippeket végigcsinálod és megfogadod a tanácsaimat, akkor valószínűleg hosszabb ideig és felszabadultabban tudod majd használni a jelenlegi számítógépedet.

Szívesen várom a visszajelzéseket és az építő kritikát is akár e-mailben (scheibj@sch-tech.hu), akár a honlapomon (http://www.sch-tech.hu) keresztül.

Ha kérdésed vagy észrevételed van a könyvvel kapcsolatban, látogass el a honlapomra.

Mindenkinek sok sikert kívánok a Windows XP biztonságos használatához!

Üdvözlettel,
Scheib János