

A hálózati szolgáltatások igénybevételének feltételei és szabályai

Minden egyes fentebb említett szolgáltatásnak saját szabályzata van. A szerzői jog értelmében ezeket a szabályokat kizárólagosan ő szabhatja meg, és változtathatja meg. A szolgáltatás igénybevételéhez általában el kell fogadnunk egy nyilatkozatot (pl. adatvédelmi), amit a mai ember jóhiszeműen egy kattintással elintézik... De végül is kinek van ideje végigolvasni? Időnként felkérnek egy-egy jogászt, aki alaposan végigmagyarázza az ott leírtakat, és akkor mindenki csak ámul...

Etikett és netikett a hálózati munka során

netikett (internetes etikett): az internetet használók legfontosabb **illemtani szabályainak** gyűjteménye. Igaz, hogy az internet a nagy szabadság egyik megnyilvánulása, de itt is szükség van bizonyos íratlan szabályok betartására.

Példák a netikett irányelveire:

Fontos a vitafórumokon való kulturált **hangvétel** megválasztása. Gyakran okoz félreértést, hogy sokan elfelejtik, egy leírt mondatot sokféle hangsúllyal fel lehet olvasni, gyakran különböző jelentéstartalommal. Ezen segítenek a smiley-k.

Ne éljünk vissza azzal, hogy a vitapartner fizikailag úgysem tud visszavágni.

A netikett a hálózat használatával kapcsolatban mondja azt, hogy mivel a hálózat közös terület, az adatátviteli

sebesség korlátozott, ne terheljük le feleslegesen, mert mindenki munkáját megnehezítheti. Az internet nagy sikerének egyik záloga az volt, hogy **nonprofit** alapon működik.

NE ÍRJ CSUPA NAGYBETŰVEL, mert az kiabálásnak számít, használj kis- és nagybetűket is chaten! Ne sértsd más vallási és hazájához fűződő érzelmeit!

Tilos flame-elni, azaz sok értelmetlen hozzászólással rövid időn belül terrorizálni a fórumot. A durva beszédet sem értékelik a moderátorok.

Általában az egyes fórumokhoz tartozik **fórumszabályzat** is, ami az adott fórum egyéni szabálygyűjteményét tartalmazza. Ezek betartása kötelező, a szabályzat figyelembevétele szankciókat vonhat maga után az egyes moderátorok-tól, adminisztrátoroktól, supervisoroktól, pl. warning (figyelmeztetés), banning (felhasználó törlése a fórum adatbázisából), esetleg időbeli korlát (pl. 10 nap), ameddig nem szólhatunk hozzá a fórum témáihoz.

Az információ értéke és hitelessége

Értéke: Adott információ értékkel bír (pl. bróker számára egy fontos üzleti döntés ténye). Az információ értéke attól is függ, hogy mennyire számít annak **frissessége**, hiszen egy adott online portál egy évvel ezelőtti híreire már alig pár ember kíváncsi. Míg ha 'szombat éjjel leszállnak az idegenek Nyírbogdány mellett', arról a lapzárta és a hétvége miatt

nem tud tudósítani az offline sajtó, ezzel szemben az online újságok akár élőben is közvetíthetik az eseményt, meginterjúvolhatják a szemtanúkat, másnap reggel pedig publicisztikák jelenhetnek meg az esemény jelentőségéről, míg a napilapok csak hétfő reggel tudnak beszámolni a történetekről. Ebben az esetben az információ értéke a frissességében van.

Hitelessége: az információ akkor hiteles, ha hozzáértő, **megbízható forrásból** származik. Az MTA honlapja valódi tudományos kérdésekben jóval megbízhatóbb, mint egy bulvárlap honlapja; a Révai lexikon egy szócikke is inkább közelebb van a valósághoz, mint egy Wikipedia-cikk, mivel azt garantáltan szakértő emberek szerkesztették. Bár a Wikipedia (főleg angol nyelven) manapság már annyira fejlett, a cikkek annyiszor lettek felülvizsgálva, alátámasztva, források megjelölve, hogy a „Wikipedia nem forrás!” kifejezést lassan elfelejthetjük.

Az álinformációk (pl. hoax) célja, felismerése, kártékony hatása és kezelése

hoax: **átverés**, tréfa, **rémhír**

Az interneten folyamatosan terjednek az számítógépes vírusokról szóló leírások, definíciók. A valódi vírus leírások, veszélyre figyelmeztető levelek közé számítógépes hoaxok is vegyülnek. Bár ezek nem fertőzik meg a számítógépes rendszereket, mégis időt és pénzt rabolnak azáltal, hogy hamis információ terjesztésére (s így pl. a hálózatok felesleges terhelésére) veszik rá a gyanútlan, jóhiszemű felhasználót.

Általában elmondható, hogy a hoaxok leleplezése, és a rémhír terjedésének megakadályozása sokkal több időt és energiát emészt fel, mint a valódi vírusok okozta káresetek kezelése.

A hoax terjedését a felhasználók jóhiszeműsége biztosítja. Ezt a jóhiszeműséget használja ki a „szaporodásra”. A leggyakoribb eset, amikor a hoax egy **email**-en keresztül (vagy közösségi oldalon) megkéri a felhasználót, hogy küldje tovább a levelet ismerőseinek, hogy ők is értesülhessenek az (amúgy hamis, nem létező) információról, vírusról, valamilyen veszélyről.

A hoaxok egy másik célja lehet a szaporodáson kívül a **szándékos károkozás**. Ebben az esetben is a felhasználó közre-működését kéri egy emailen keresztül, ahol például az található, hogy a Microsoft egy újabb biztonsági rést talált a rendszerén, és ez úgy orvosolható, ha parancssorban kiadjuk a `format c:` parancsot. Egy ilyen üzenet a hozzá nem értő számára egyáltalán nem tűnik gyanúsnak, sőt a levél tovább fokozza a hitelesség látszatát azáltal, hogy egy nagynevű cégre hivatkozik. Ezek az incidensek könnyen kiszűrhetők lennének a megfelelő oktatással melyeknek költsége eltörpül az okozott kár következményeként jelentkező bevételkiesés mellett.

Néha informatikai biztonságtechnikával foglalkozó cégek, vagy vírusellenes szoftverek fejlesztői is kibocsátanak figyelmeztető felhívásokat, ám ezek eredete minden esetben tisztázottnak vehető (pontosan tudható, ki vagy kik indították el, sokszor a kibocsátó saját **PGP** (Pretty Good Privacy) **kulcsával** is aláírja ezeket hitelesíthetőség céljából).

Az azonosításhoz előbb szükséges megismerni a hoaxok működését, valamint azt, hogy mit csinál a sikeres hoax az interneten. A sikerének két tényezője van:

A számítógépes szakzsargont használja A hitelesség látszatát kelti

Ha a figyelmeztetés bizonyos technikai szakzsargont használ, akkor a legtöbben, még a szakemberek is, hajlamosak valódinak hinni. Például a Good times hoax a következőt tartalmazza: „... ha a program nem áll le, a processzor végtelen ciklusba kerül, és ez súlyosan károsíthatja azt...”

Ez első ránézésre hihetőnek tűnhet a hozzá nem értő felhasználó számára, de nyilvánvaló, hogy egy processzor nem károsodik önmagában a végtelen ciklustól.

Különös éberségre int az, ha a figyelmeztetésben hangsúlyozzák a **továbbküldés fontosságát**. Ez a hoax legfontosabb ismérve.

A legegyszerűbb módszer az ilyen körlevelek elkerülésére, hogy mielőtt továbbküldi a bizonytalan felhasználó, **ellenőrizi a hitelességét**. Erre alkalmas módszer, ha megkérdezi rendszergazdáját vagy erre specializálódott cégek szakembereit. A valódi figyelmeztetések vírusokkal és egyéb hálózati problémákkal kapcsolatban általában a következő szervezetektől érkehetnek: pl. CIAC, CERT, ASSIST, NASIRC, vagy bármely antivirus fejlesztő cég, és többnyire PGP digitális aláírás van rajtuk. A névtelen üzenetek, vagy azok, amelyek nem létező címet, telefonszámot tartalmaznak, nagy valószínűséggel hoaxok.

Az információszerzés és a publikálás legális és illegális formái

Publikálás: Adott ország törvényeitől függ, de általában mindenhol tilos az illető jóváhagyása nélkül róla és környezetéről adatokat gyűjteni és azt felhasználni vagy továbbadni. Itt fontos bevezetni azt a fogalmat, hogy **intellectual property**, azaz szellemi tulajdon, mivel annak megsértése és az azzal való visszaélés nem csak a plágium kérdését veti fel, hanem a törvény is bünteti. Szabadalmaztatott programokat, eljárásokat, levédett filmeket, zenéket, képeket, szövegeket tilos saját nevünk alatt saját oldalunkon publikálni esetleges licencszerződés vagy hozzájárulás nélkül.

Információszerzés: Legális információszerzés, ha kérdőívekkel, interjúkkal, fórumon kommenteléssel, emailben (nem spamben!), személyesen megkérdezzük. Illegális, ha a másik tudta nélkül, pl. pendrive-jának/laptopjának ellopásával vagy arról adatok elemelésével, keyloggerrel, lehallgatással, stb. tudunk meg valamit. A **P2P** (peer-to-peer, fájlmegosztás) hálózatokról (bár a P2P nem illegális!), tehát fájlcsereelő szerverekről – Napster (kezdetben), BitTorrent –, fájl-csereelő programok (µTorrent) segítségével szintén illegális védett fájlokat, zenéket, filmeket letölteni, ugyanakkor legális saját készítésű fényképeinket, dokumentumainkat megosztani. De ez már a warez (jogsértő tartalmak terjesztése) kérdése.