Ergonómia

A számítógép állandó használata egészségkárosító hatású. A számítógépek munkahelyi használatát törvény szabályozza, mind időben, mind a munkahely kialakításában:

- A közvetlen napfény erősen rontja a képernyő láthatóságát.
- A monitor üvegén levő tükröződés rontja a láthatóságot / koncentráltságot.
- Az árnyékban levő monitor előtt dolgozó felhasználó szemébe tűző nap is rontja a szemet.
- Az ideális munkahely a kezességgel szembeni oldalról kapja szűrve a napfényt, miközben a monitor árnyékban van.
- Mesterséges világítás legyen szórt, a munkaasztalon irányított.
- Az irodai bútorok állítható magasságúak legyenek, hogy ne kelljen kicsavart testhelyzetben, vagy görnyedve dolgozni.
- Ne alakítsunk ki munkahelyet számítógépes klaszter közepén (igen zajos)
- Az ergonomikus számítógép lehetővé teszi a használatával együtt járó munkahelyi megterhelések, illetve baleset- és munkavédelmi veszélyforrások kiküszöbölését, vagy előfordulásuk megakadályozását. Ezeket az elvárásokat a svéd Tjänstemännens Centralorganisation (TCO) által kidolgozott szabvány foglalja össze.

Veszélyforrások:

- Monotonitás (merev testtartás, feszült figyelem: izom-, hát-, nyaktájéki fájdalmak, izongörcsök, vérkeringési zavarok, szívfájdalom)
- Kivédése: 50 percenként 10 perc szünetet tartva rendszeres mozgást végezzünk. Ha van rá lehetőség, munkánkat úgy szervezzük, hogy változó jellegű tevékenységet végezzünk.
- Billentyűzet és egér használata: kritikus a testtartásra, ínhüvelygyulladást, vérkeringési zavarokat okozhat a nem megfelelő beállítás. Ez fokozottan jelentkezik a hordozható gépek nem teljes méretű billentyűzetén.
- A probléma oka: a hagyományos billentyűzet használatakor az emberek 5 fokot előredőlnek. Igyekezzünk minimalizálni a billentyű- és egérhasználatot (gyorsbillentyűk, makrók), rendszeresen mozgassuk végtagjainkat.
- Az ergonomikus billentyűk (íveltek, középen kettényithatók és tetszőleges szögben állíthatóak) képesek a testtartás megváltoztatására (15 fok hátrahajlás), viszont hatékony használatukhoz két kézzel kell megtanulni gépelni.
- Egér: a karunk az asztalon pihenjen, és csak a csukónk mozogjon. Az egérmozgató szoftvert úgy célszerű beállítani, hogy az egér 5x5 cm-es mozgása lefedje a képernyőt.
- Képernyő: manapság már kezdenek kimenni a divatból a katódsugárcsöves készülékek. Célszerű nagyobb frekvenciájú (képernyőfrissítés) monitort használni, mivel a villogás fárasztja a szemet.
- Nyomtatók: zajterhelés problémák, nem célszerű egy központi nyomtató mellett dolgozni. Lézernyomtatók esetén szempont az alacsony ózonkibocsátás is.

Szotfverergonomia

- „Barátságos” felület
- Jó dokumentáltság (könnyen visszakereshető referenciatáblák, interaktív súgók, stb.)
- A lényeg, hogy megfelelő komfortérzetet keltsenek, csökkentsék a helytelen adatbevitelből, kezelésből eredő hibák valószínűségét, biztosítsák a szolgáltatások teljes körű felhasználását.
- Ezekre a feltételekre igazából csak a 90-es évektől figyelnek a szoftvergyártók, amióta a számítógépes szoftver igazi tömegcikk lett.
- Programokkal szembeni elvárások:
    - Megbízhatóság (feladat „tökéletes” ellátása, az illetéktelen felhasználás kizárása)
    - Könnyű kezelhetőség (áttekinthetőség, súgók, egyéni beállítások)
    - Felhasználóbarát adatbevitel (alapértelmezés felajánlása, ellenörző szűrők, ismétlődések kizárása, jó összesítés megjelenítés)
    - Könnyű karbantarthatóság és továbbfejlesztés (makrók, programozás)
    - Adaptív felületek: a program alkalmazkodik a felhasználói szokásokhoz – pl. a menükben a felhasználó által gyakran használt elemek jelennek meg elsődlegesen). Másik módszer az objektumok (pl. ikonok) kinagyítása, ha fölöttük van az egér.

Információs társadalom

- Az számítógép és a számítógépes hálózat megváltoztatta az életünket, és az emberek egymáshoz való viszonyát is:
    - A keresők révén a bőséges információ könnyen és gyorsan elérhető (ismeretek megszerzése, megosztása)
    - A különböző fórumok hatékonyan önszervező módon terelik egybe az adott témában érdeklődőket (ez veszélyeket is rejt, terroristák is szívesen használják).
    - Rádöbbentünk a „kis világ”-ra: tetszőleges két ember 5-6 baráton, ismerősön keresztül megtalálja egymást.
    - Krízishelyzetekben is hatékonyan tud híreket eljuttatni (ld. balkáni háború internetes közvetítése).
    - A társadalom „függővé” válik a számítógépektől, a 2000-es év problémájára igen alaposan készültek; a számítógépek leállása repülőtereken, TV-kben, bankokban, államigazgatásban megbénítja azok működését.

Információvédelem

Számítógépen tároljuk rengeteg személyes adatunkat (magánszemélyek, cégek, államigazgatás). Ezeknél lényeges, hogy

- folyamatosan rendelkezésre álljanak
- illetéktelenek ne férjenek hozzá

Az információvédelem eszközei:

- A hozzáférés-jogosultság rendszer kiépítése és üzemeltetése
- Hozzáférés-ellenőrzés
- Nyilvántartási rendszer (ki mikor mit csinált)
- Megbízható működés, adatok sértetlenségének és konzisztenciájának biztosítása
- Szisztematikus, rendszeres adatmentés
- Szoftver- és hardverhibák ellenőrzése és elhárítása
- Sérült adatok gyors helyreállítása.
- Az adatok érzékenységi szint szerinti osztályozása és kezelése
- Felhasználók egyedi azonosítása és jogosultságaik pontos megadása

Támadások személyes adatok ellen:

- Spyware
- Banki honlapok hamisítása (phising)

Vírusok

A számítógépes vírusok olyan programok, melyek a rendszerbe engedély nélkül belépve, ünmagukat másolják, többszörözik, és más programokat megfertőznek. A vírusok jó része ezen kívül valamilyen esemény hatására, vagy adott időpontban aktiválódva más károkat is okozhat.

A vírusok az informatika fejlődésével folyamatosan fejlődnek. Fő típusaik:

- **Boot vírus**: az első vírusok közé tartoznak, fertőzött (hordozható) lemezről terjednek. A vírus a merevlemez boot (indulási) szektorába épül be, és az operációs rendszer indulása előtt aktiválódik. A fertőzött merevlemez az összes meghajtóba helyezett lemezt megfertőzi. Manapság a kevésbé elterjedt vírusok közé tartozik.
- **Programvírusok**: a futtatható állományokba ágyazódnak be. Amikor a fertőzött programot elindítjuk, az a memóriába töltődik, és átterjed minden futtatott programra. A gépünkre legtöbbször úgy kerül, hogy valaki rávesz minket a futtatására (másolva kapjuk, vagy hálózatról töltjük le).
- **Makróvírusok**: az Internet elterjedésével szaporodnak el. A makró egy dokumentum, vagy táblázatkezelő gyakran ismételt lépéseire írt egyszerű program, mely elszabadulva nagy kár tud okozni a rendszerben. Szintén megosztás révén terjed.
- **Férgek**: az Interneten terjednek, kihasználva a hálózati programok gyenge pontjait. Főképpen a levelezőrendszeren keresztül jutnak be, és kiolvasva a címjegyzékünket automatikusan továbbküldik magukat az ott levő címekre.
- **Trójai faló**: olyan önálló alkalmazások, melyek ránézésre hasznos tevékenységet fejtenek ki (esetleg adatvédelmet), de kártékony kódot tartalmaznak.

Virusok két fő csoportja:

- **Lopakodó vírus**: állományba ágyazódnak, onnan futtatáskor a memóriába kerül. A ravaszabbak arra is ügyelnek, hogy az állomány eredeti méretét mutassák, illetve az eredeti ellenőrzőösszeget szimulálják.
- **Polimorf vírusok**: önmagukat titkosítják változó módon. Mivel a vírusfelismerő programok a vírust a „mintázata” révén ismerik fel, ez jelentősen megnehezíti a vírusok felismerését.

Védekezés:

Megelőzés:

- Rendszeres mentés (hogy visszaállítható legyen az utolsó nem fertőzött állapot)
- Beérkezett adatok (levél, külső lemez) használat előtti ellenőrzése
- Rezidens vírusirtók telepítése
- Jogtiszta, ellenőrzött forrásból származó szoftverek

Jogi tudnivalók

- Az Interneten rengeteg információ (adat, kép, hang, videó, program, stb.) érhető el, de ez nem jelenti automatikusan, hogy azok szabadon fel is használhatók.
- A felhasználhatóság korlátozását általában külön jelzik (copyright)
- Publikálás esetén mi is jelezzük, hogy ki a tulajdonjog birtokosa, és milyen módon használható fel az információ.
- Személyes adatok védelme (1992. évi LXIII tv. – Avtv.) szerint személyes adat csak akkor kezelhető, ha ahhoz az érintett hozzájárult, vagy azt törvény, illetve helyi önkormányzat rendelete előírja.
- Az internet szabályozása felépítéséből következően nehézkes:
    - nemzetközisége miatt ellentmondásban lehet egyes országok szabályzásával (pl. titkosítások),
    - törvény által nem kategorizált részei ellentmondásban lehetne médiatörvényekkel,
    - névtelen szolgáltatásai törvénysértésre adnak alkalmat,
    - technikai fejlődése mindig új helyzet elé állítja a törvényalkotókat.
- Ha programot teszünk közre, arról minden esetben nyilatkozni kell, hogy ki használhatja fel (pl. bárki), és milyen felelősséget vállalunk érte (pl. semmilyet sem).
- Törvénysértő adatok közlése, adatok törvénysértő megosztása (fájlcserélők, vírusok, spamek) az interneten különböző jogi következményeket vonhat (és volt is rá példa az ELTEn) maga után.
- Minden ELTE hálózati felhasználóra érvényes az ELTE hálózati szabályzata.

Szortverek

A legtöbb jogsértés a szoftverekkel történik A szoftverek a következő kategóriákban sorolhatók:

- **Freeware**: szabad szoftver, ingyen beszerezhető és használható, általában korlátlan ideig. A legtöbb esetben a GPL (Gnu Public License) látják el, és ennek értelmében pénzért továbbadható -- amennyiben valaki hajlandó pénzt adni érte.
- **Shareware**: olyan program, mely korlátozott ideig használható fel ingyenesen (demo időszak), illetve ingyenes változata nem a teljes funkcionalitást biztosítja, de kipróbálás után a fizetős változatát megrendelve már korlátlan ideig felhasználható teljes értékű változatot kapunk.
- **Béta szoftver**: egy szoftverfejlesztés utolsó előtti fázisában levő szoftver, mely még jelentősebb hibákat is tartalmazhat, de felhasználását a fejlesztő ingyenesen lehetővé teszi (általában korlátozott ideig). Fő célja, hogy a terméket minél többen próbálják ki, ismerjék meg és teszteljék le. A végső változatot meg kell vásárolni (esetenként a legjobb béta tesztelők ilyenkor ingyen kapják meg a végső változatot).