Internet felelős és etikus használata

A XXI. század új információ csatornája az Internet, melynek létrejöttét a technikai civilizáció fejlődése tette lehetővé. Az új média segítségével az információk a korábbiakhoz képest sokkal több helyről sokkal több emberhez jutnak el sokkal gyorsabban, mint bármikor korábban, legyőzve teret és időt. Egy könnyen kezelhető, kisméretű, az átlagember számára is megfizethető hordozható eszközzel, a Föld bármely helyén elhangzó élőbeszéd, szónoklat, zene, színjáték, esemény késedelem nélkül hallgatható, nézhető. Költséges nyomdatechnikától, papírgyártástól, és könyvtár épületektől függetlenül óriási mennyiségű nyomtatott könyv, újság, szakcikk digitális változata olvasható, rádió és televízió állomások adásai követhetők a vételükhöz korábban szükséges nagyméretű helyhez kötött készülékek nélkül. Az információ csatornák nyilvánosak, a hozzáférés kényelmes, és demokratikus, ennek minden előnyével és hátrányával. Létrejött egy új társadalmi dimenzió: ONLINE. Meglepődve jelenthetjük ki, a történelmi kor emberének volt egy jelzője, amiről nem is tudott: Hogy vagy? – OFFLINE!

Digitális kompetencia

Az online kapcsolattartás formáinak fejlesztése elsősorban a mobil telefonálásra használt eszközökön keresztül, különösen az egyes élethelyzetekre kifejlesztett alkalmazások segítségével történik. Hivatalos ügyek, utazással kapcsolatos teendők, vásárlás, szállásfoglalás… mind gyakrabban bonyolítjuk ezeket az online térben. A digitális kompetencia így általános szükségletté vált.

Információ relevancia

Az interneten elérhető információk relevanciájának (helytállóságának) mértékével kapcsolatban különböző becslések léteznek. Az értékek 50% és 65% között mozognak a számítási módszer függvényében. A relevanciába beleértjük a szolgáltatott információ igazságtartalmát és azt is, a kérésünknek megfelelő tartalmat szolgáltatott-e az online keresőmotor.

Személyiségi jog

A személyiségi jogok az online térben is megilletik az embereket. Különösen a *jó hírnév*hez való jog, a *magántitok*hoz és a *személyes adatok*hoz való jog, illetve a *szellemi tulajdon*hoz való jog. Minden olyan adatot, amellyel egy személyt beazonosíthatunk személyes adatnak kell tekinteni, ezen belül különleges adatnak számit például a politikai nézet, vallás illetve az egészségi állapot.

Internet etikett

Ahogy az „offline” térben, úgy az online térben is vannak írott és íratlan szabályok, melyeket be kell tartani. Az offline térre vonatkozó szabályok kiegészülnek e specifikus online média sajátos viselkedési szabályaival. A legáltalánosabb elv, hogy se magunkat, se másokat ne hozzunk veszélyes, kellemetlen vagy jogsértő helyzetbe, előzzük meg az ilyen eseteket.

Veszélyek az online térben

Az emberek számára természetes, hogy a hétköznapi életben (az „offline” térben), nem ismerkednek meg ellenszenves idegenekkel, személyes élményeiket csak ismerőseikkel, barátaikkal osztják meg, védik személyes tárgyaikat, tulajdonukat. Az online tér „arctalansága” ugyanakkor könnyelművé teheti a felhasználót. Ráadásul az internetes technológiák fejlődése számtalan veszélyes eszközt ad a rosszindulatú hackerek kezébe.

Email fiók feltörése

Ismeretlen e-mail sürgősnek tűnő üzenetet tartalmaz, vagy olyan üzleti ajánlatot, amely kihagyhatatlannak látszik. Ha a levélben szereplő hivatkozásra kattintunk, előfordulhat, hogy egy káros kódot tartalmazó weboldalra jutunk, amely megpróbál betörni számítógépünkre, feltörve e-mail fiókunkat. Így ismeretlenek megszerezik jelszavainkat, levelező partnereink e-mail címét, elolvassák leveleinket, megnézik csatolt állományainkat.

Érdeklődési kör, fogyasztási szokások meghatározása

A hirdetési és reklám oldalak marketing céljából információ-kereséseink alapján rögzítik érdeklődési körünket, fogyasztási szokásainkat.

Profilalkotás

A „Like” gomb használata felhasználói attitűdjeinket, netes viselkedésünket teszi követhetővé a közösségi oldalakon. Az úgynevezett „clickjacking” (≈ klikkelésbe bújtatott like) hasonló eszköz. Pl. amikor egy megnézni kívánt videóra kattintunk, valójában egy láthatatlan „Like” gombot nyomunk meg, még akkor is, ha a video tartalmat nem értük el. A legújabb technológiák képesek elemezni egérhasználatunkat is. Az intelligens eszközökre telepített szoftverek legtöbbje megkérdezésünk nélkül adatokat küld a gyártó honlapjára az eszközünkről. Ezt legtöbbször telepítéskor az EULA (végfelhasználói licensz szerződés) is közli a felhasználóval: *„… Előfordulhat, hogy a/az ..... (gyártó) adatokat küld az Ön eszközéről a/az ..... (gyártó) központi web helyére. ... ”*

Tartózkodási hely meghatározása

Amikor böngészőnk segítségével belépünk egy web oldalra, az oldalon található információ megjelenítéséhez közölni kell az információt tartalmazó szerverrel webcímünket a kért információ gépünkre juttatásához. A strukturált webcímek alapján azonban könnyedén meghatározható helyzetünk akár ország-város- utca-házszám dimenzióban is.

Intelligens eszköz jogosulatlan használata táveléréssel

Az úgynevezett távelérési technikákat (remote control) eredetileg azért fejlesztették ki, hogy egy-egy intelligens eszköz (pl. számítógép, mobiltelefon, műholdas beltéri egység, tablet stb.) meghibásodott szoftverének javítását, frissítését távolról is meg lehessen oldani. Ezek a technológiák alkalmasak arra is, hogy jogosulatlan személyek intelligens eszközünk kamerájának, mikrofonjának vezérlését vezetékes vagy wi-fi technológiával átvegyék, és környezetünkről tudtunkon kívül adatokat szerezzenek.

Bankkártya adatok eltulajdonítása

Internetes vásárlás esetén választhatjuk a „fizetés bankkártyával” opciót. Egy körültekintően tervezett és konfigurált weboldal ilyenkor felajánlja, hogy adatainkat titkosítva, *https* protokoll használatával forgalmazza. Még ekkor sem lehetünk azonban teljes biztonságban. Néhány évvel ezelőtti történet, melyet a napi sajtó is megírt: hackerek egy bank honlapjára megtévesztésig hasonló honlapot készítettek. A gyanútlan felhasználókat a bank honlapjára kattintás után saját áloldalukra navigálták, majd egy hihetőnek tűnő „biztonsági okra” hivatkozva kikérték az ügyfelek bankkártya adatait. Több százan vesztették el bankba tárolt pénzüket. (a támadott bank nevét, illetve a keletkezett kár mértékét nem hozták nyilvánosságra)

Internet függőség

Valós környezetünkkel kapcsolatos felfogásunkat, érzékelésünket, hozzáállásunkat, szokásainkat, akár személyiségünket is károsan formálhatja az állandó online jelenlét, függőséget okozva. Ennek a veszélynek különösen a gyerekek vannak kitéve, akik koruknál fogva nem tudják kellően megkülönböztetni egymástól a valós és virtuális világot.

Felelős használat

Internetezésre használt eszközeink biztonsági beállításaival, megfelelő tűzfalvédelem és vírusvédelem kialakításával, ismereteink bővítésével, elővigyázatos magatartással előzzük meg, hogy vírusok, rosszindulatú programok kerüljenek az eszközeinkre. Korlátozzuk a személyes jellegű, bizalmas, illetve indokolatlanul részletes információk megosztását, ne hozzuk ezeket akaratlanul nyilvánosságra. Válasszuk meg, mely weboldalakat látogatunk meg, a bejelentkezésekhez használt jelszavainkat gondosan őrizzük, ne adjuk át másoknak.

A tűzfal, illetve a böngésző alkalmazás részletes konfigurálására ne sajnáljuk az időt! Tiltsuk le a helymeghatározás lehetőségét, ne vagy csak minimális mértékben engedélyezzük a nyomkövető (tracer) technikák használatát. Aktiváljuk böngészőnk adathalászat ellen beépített védelmét. A böngésző ekkor ellenőrizni fogja a meglátogatott oldalakat, adathalászatra jellemző események után kutatva, és figyelmeztetést küld, ha ilyet észlel.

Ingyenes alkalmazások letöltése előtt mérjük fel az applikáció használatával járó esetleges veszélyeket. Amennyiben az EULA-ben „gyanús” dolgokra bukkanunk, ne használjuk a szoftvert, váltsuk ki megbízhatóbb alkalmazással.

Az egyes hardveres szolgáltatások saját szabványos port címmel rendelkeznek. Például a nyomtató szolgáltatás is egy szabványos port számon kommunikál. Ha soha nem használunk egy bizonyos szolgáltatást, tiltsuk le a hozzá rendelt port szám használatát. Ha ritkán használjuk, rendeljünk parancsikont a szolgáltatáshoz, amelyet az asztalon helyezünk el. A használat idejére ezután könnyen tudjuk engedélyezni a port megnyitását. Hasonlóan járjunk el a vezetékes illetve wi-fi kommunikációs portokkal. Ezzel jelentősen megkönnyítjük a tűzfal munkáját, illetve megnehezítjük a vírusok bejutását intelligens eszközünkre. Amennyiben nem akarunk élni a távoli hozzáférés lehetőségével tiltsuk le a szolgáltatást.

Bankkártyás fizetés előtt, a bank online alkalmazása segítségével hozzunk létre virtuális számlát, belső utalással utaljunk virtuális számlánkra akkora összeget, amire szükségünk lesz, és a virtuális számlán keresztül fizessünk az online térben.

Ha nem ellenőrzött (not certified) oldalról töltünk le információkat, több forrásból is ellenőrizzük azok hitelességét.

Jogi védelem

A médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény rendelkezései alapján un. Média-és Hírközlési Biztos közreműködik az elektronikus hírközlési szolgáltatást, illetve a médiaszolgáltatást igénybe vevő felhasználókat e szolgáltatások igénybevétele körében megillető, méltánylást érdemlő érdekek érvényesülésének elősegítésében.

Jogsértés esetén bírósághoz fordulhatunk, ahol kérhetjük a jogsértés bírósági megállapítását, a jogsértés abbahagyását vagy a jogsértő eltiltását a további jogsértéstől. Kérhetjük, hogy maga a jogsértő adjon valamilyen elégtételt. Jogkövetkezményként követelhető a sérelmes helyzet megszüntetése, a jogsértést megelőző állapot helyreállítása és a jogsértéssel előállított valós vagy virtuális termék megsemmisítése vagy jogsértő tartalmától való megfosztása. Súlyosabb esetben a jogsértés következménye akár büntetőjogi felelősségre vonás is lehet.

Etikus használat

Toleráljuk, ha embertársaink az online térben szenzációsnak, közérdekűnek, bájosnak, viccesnek vélt tartalmakat tesznek közzé, számukra fontosnak tűnő dolgokhoz való csatlakozásra buzdítanak, vagy számukra fontosnak tűnő elvekkel való azonosulást várnak el. Hagyatkozzunk józan ítélőképességünkre, belátásunkra, mennyiben értünk egyet a közölt tartalmakkal. Ugyanakkor kerüljük a számunkra érdektelen, zavaró, esetleg jogszerűtlen tartalmak további megosztását.

Ne küldjünk másoknak sértő illetve bántó üzeneteket, ne állítsunk másokról valótlanságokat. Más személyről képet, hangfelvételt csak az érintett beleegyezésével lehet megosztani.

Levelek továbbküldésénél (forward) ne változtassuk meg annak szóhasználatát. Ne továbbítsuk más e-mail címét harmadik személy felé az érintett megkérdezése nélkül.

Ha online fórumhoz csatlakozunk, először tekintsük át a fórum használói által elfogadott szabályokat. Ne adjuk ki sem saját, sem ismerőseink személyes adatait. Mi se kérjük másoktól ugyanezt. Beszélgetés közben ne alkalmazzunk bántó nyelvezetet.