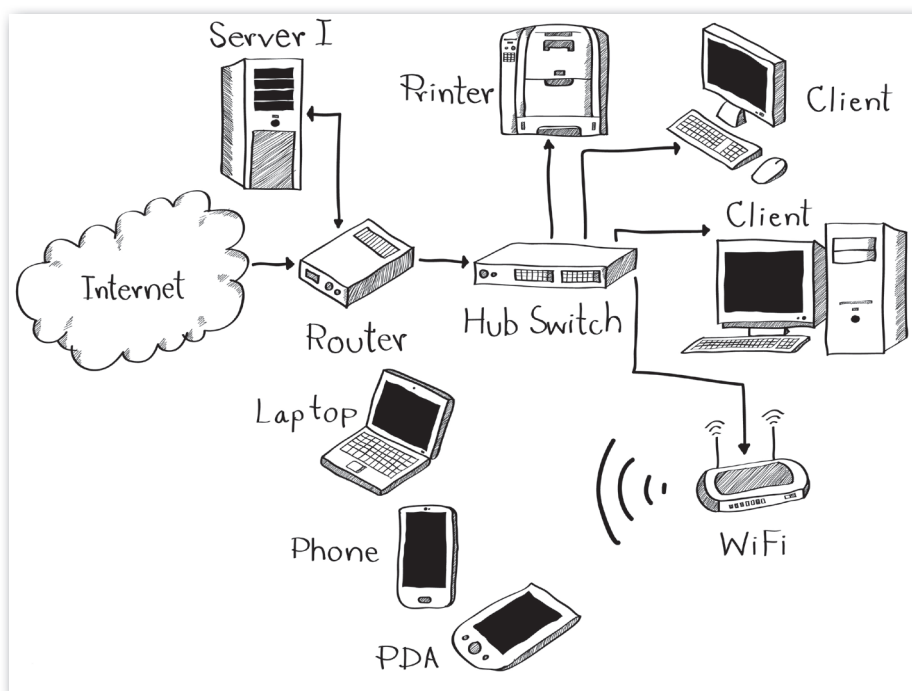


Felhőszolgáltatások, felhőalkalmazások

A felhőről tudjuk, hogy valójában olyan számítógépeket jelent, amelyekről legfeljebb sejtjük, hol vannak, de nem tudjuk, hogy mekkorák, milyen erősek, és azt sem, hogy pontosan milyen szoftverek futnak rajtuk. Azzal viszont tisztában vagyunk, hogy ezekkel a számítógépekkel, pontosabban a rajtuk futó alkalmazásokkal a világ legnagyobb számítógépes hálózataán, az interneten keresztül a mi eszközeinken futó alkalmazások kapcsolatba tudnak lépni. Így lehetőségünk nyílik a felhő szolgáltatásainak, a felhőben futó alkalmazásoknak a használatára.



► Emlékszünk még, hogy honnan ered a „felhő” elnevezés?

Feladat

Gyűjtsünk össze olyan alkalmazásokat, amelyek a felhőben futnak, és amelyeket használhatunk vagy használhatnánk! Alighanem azt látjuk, hogy ezek az alkalmazások jó része besorolható a következő csoportokba:

- adattárolók és megosztók (ideértve a fotók, videók, hangok, prezentációk megosztását is);
- kapcsolattartók;

- c) ügyintézésre használhatók (például az időpontfoglaló vagy az adóbevallásokkal, iskolai felvételikkel, közművekkel kapcsolatos ügyintézésekre lehetőséget adó felhőalkalmazások vagy a bankok oldalai);
- d) vásárlásokra használható weboldalak;
- e) tájékoztatásra használatos oldalak (akár az iskolánk honlapja, akár a Wikipédia, akár egy internetes újság, akár egy program használatával vagy a tavaszi fametszésekkel foglalkozó weboldal);
- f) játékszerverek, amelyekhez egy-egy számítógéppel, okostelefonnal kapcsolódva közös játékban vehetünk részt;
- g) alkotómunkára használható weboldalak (például a sokak által használt internetes szövegszerkesztők, a fotók retusálására vagy hanghatások előállítására használható oldalak stb.);
- h) olyan alkalmazások, amelyekbe valamilyen érzékelőket, kisebb eszközöket regisztrálnak, és ezeknek az interneten át közvetített adatait dolgozza fel a felhőben futó központi gép, vagy ezek az eszközök vezérelhetők vele (idesorolhatók például a telefonos térkép- vagy a vonatok aktuális helyzetét nyilvántartó alkalmazások, de például azok is, amelyek egy hatalmas gyártelepen vagy a plázákban felszerelt hőmérők és légnedvességmérők adataiból rajzolnak grafikonokat az épület üzemeltetőinek);
- i) tanulásra alkalmas weboldalak, alkalmazások.

Feladat

Soroljuk be a fenti csoportok valamelyikébe az összegyűjtött szolgáltatásokat! Ha egyikbe sem sikerül elhelyezni egy-két alkalmazást, akkor gondolkodjunk el: lehet, hogy léteznek további csoportok is? A besorolás nem mindig egyértelmű. Hova kerül egy vasúti menetrend vagy a színház, a cirkusz és a szabadidőpark oldala, ahol jegyet is vehetünk? Hova sorolhatók az előfizetéssel látogatható internetes televízió- és rádióadók oldalai?

Weboldal, honlap = felhőalkalmazás?

Ennyire egyértelműen azért ezt nem lehet kimondani. A kétséget részint az okozza, hogy az internet első évtizedében (azaz a múlt évezredben) a weboldalak többnyire olyanok voltak, mint egy-egy elektronikus hirdetőoszlop vagy faliújság. Elolvasható információkat, megnézhető képeket és letölthető fájlokat (programokat, hosszabb szövegeket, zenéket) helyeztek el rajtuk.

A tartalmakat mindig a honlapok üzemeltetői töltötték fel, a látogatók nem tudtak beleavatkozni vagy tartalmat elhelyezni rajtuk. A feltöltött hangokat előbb le kellett tölteni, és egy, a számítógépre telepített hanglejátszó alkalmazással lejátszani. A böngésző erre alkalmatlan volt. Videók letöltésére nagyon



- ▶ A felhőt alkotó számítógépek nagy része különleges épületekben, adatközpontokban kap helyet. Egy adatközpontban sok-sok ezer számítógépen futnak különféle programok, például az általunk is használt webes szolgáltatások. Adatközpontokban lévő számítógépekre kerülnek a „felhőbe” mentett adataink is

ritkán volt lehetőség, és akkor is rövid és kis felbontású felvételeket tartalmazó fájlokról volt szó. Akkoriban kevés volt a gépekben a háttértár, és kicsi volt az internetkapcsolatok sávszélessége a nagyobb fájlokhoz.

Idővel ez megváltozott. A weboldalak sok éve már úgy készítik, hogy a böngészőnkben hozzá tudjunk szólni egy-egy cikkhez, vagy csevegni tudunk rajtuk egymással. A webshopok, kapcsolattartók, videómegosztók, amelyek lényegesen túllépik a kezdeti, hirdetőtábla-szerepű weboldalak képességeit, mára már a mindennapok részévé váltak. Megjelentek a webes alkalmazások, a felhőszolgáltatások és -alkalmazások, de a felhőalkalmazásoknak csak egy részéhez tudunk a böngészőnkéből kapcsolódni. A másik részükhöz speciális kliensalkalmazásra van szükség – gondoljunk csak a telefonunkban futó térképalkalmazásokra, de sok üzenetküldő is ilyen.

Kérdések, feladatok

1. Az előző feladatban felsorolt csoportok közül melyik az, amelyik nem sokat változott a múlt évezred óta?
2. A böngészőnk belsejében futó felhőalkalmazások sokszor alig különböznek a számítógépünkre telepített alkalmazásoktól, és mostanra sok esetben elég jó ahhoz, hogy ne bajlódjunk egy-egy alkalmazás telepítésével. Soroljunk fel ilyen felhőalkalmazásokat és a nekik megfelelő, gépre telepíthető szoftvereket!
3. Már jó ideje létezik olyan operációs rendszer, amelyet főként laptopokra telepítenek, és lényegében kizárólag a felhőben futó alkalmazásokat lehet vele használni.
 - a) Keressük meg, mi a neve, és nézzünk meg videókat a használatáról, működéséről!
 - b) Melyik cég fejlesztje?
 - c) Beszéljük meg, hogy miért lehet érdemes ilyen operációs rendszerrel szerelt laptopot vásárolni, és miért nem!

Adattárolás földi körülmények között és a felhőben

Ha biztonságban akarjuk tudni azt a prezentációt, amelyen hosszú órákat dolgoztunk, vagy azokat a képeket, amelyek soha meg nem ismételtető pillanatainkat rögzítik, akkor gondoskodnunk kell a megfelelő tárolásukról. Könnyen elveszíthetjük, ha egyetlen háttértáron, adathordozón tároljuk őket, hiszen ez is csak egy alkatrész, így bármikor meghibásodhat. Adataink minimális biztonságához minden fájlt legalább két helyen kell tárolnunk.

Kérdések

1. Hol tárolhatjuk a számítógépünkön szerkesztett dokumentumok, házi feladatok biztonsági másolatát?
2. Mi a teendő, ha biztonságban akarjuk tudni az okostelefonnal készített, megtartani szánt képeinket?



▶ A külső adathordozó biztonsági másolatok tárolására is jó

A biztonsági mentések történhetnek online – ekkor a mentés helyéül szolgáló eszköz (külső adattároló, pendrive, memóriakártya) folyamatosan kapcsolódik a gépünkhöz. A biztonsági másolatokat tároló online eszközök előnye, hogy egyszerűen kimenthetjük rájuk a napi munkánk eredményét – azaz nem fogjuk ellustálkodni a biztonsági másolat elkészítését. A hátrányuk, hogy ha rosszindulatú támadás (például vírus) éri a számítógépünket, telefonunkat, akkor a biztonsági mentés is tönkremehet.

Ezért szokás a fájlokat egy további eszközre (általában pendrive, egyéb külső adathordozó) is menteni – ez az offline biztonsági másolat. Ezt az eszközt csak időnként csatlakoztatjuk a gépünkhöz.

Kérdések

1. Mik az offline biztonsági másolat előnyei és hátrányai?
2. Mi szól amellett, hogy időről időre elkészítsünk ilyen másolatokat?

Ahol az adatok igazán számítanak, mert pótolhatatlanok, sok év munkája fekszik bennük, ott egy harmadik helyre is szokás biztonsági másolatot készíteni. Ez a harmadik hely elég messze található ahhoz, hogy katasztrófa (tűzvész, árvíz, földrengés) esetén is megmaradhassanak az adataink.

Mindhárom mentésre ideális lehet a felhőszolgáltatók adattároló szolgáltatásának igénybevétele. Szinte biztosan kínálnak valamilyen, az operációs rendszerhez illeszkedő, a háttérben futó alkalmazást, azaz adatainkat elég egy mappába másolni, vagy automatikusan átkerülnek például a fényképeink a felhőbe.

A felhőszolgáltatók a mentett fájloknak több változatát is megőrzik, így például nem vagyunk nagy bajban, ha véletlenül kitörölünk két oldalt a házi dolgozatunkból, és elmentjük a változtatásokat. Ilyenkor egyszerűen vissza tudjuk tölteni a fájl előző változatát. A felhőszolgáltatók számítógépeiben is meghibásodnak a háttértárak, de az adatainkat mindig több eszközre mentve tárolják, azaz nem vesznek el ilyenkor.

Kérdések, feladatok

1. A felhőszolgáltatásokkal szinte mindig ingyen tárolhatunk egy kisebb mennyiségű adatot, a többiért viszont fizetnünk kell. Miért van ez így? Nézzünk utána, mennyibe kerülnek ezek a szolgáltatások!
2. Keressünk olyan cégeket az interneten, amelyek felhőszolgáltatást kínálnak! Melyek készítenek közülük operációs rendszert is?
3. Milyen esetekben nem jó megoldás adatainkat a felhőben tárolni?
4. Mikor érdemes egy videót vagy képet adattároló alkalmazásban tárolni, és mikor van jobb helyük egy fénykép- vagy videómegosztó webes alkalmazásban?
5. Osszunk meg egy felhőszolgáltatásban a számítógépünkön lévő fájlokat, mappákat! Értessük elektronikusan a megosztott adatokról tanuló társainkat, és töltsük le a számítógépünkre azokat az adatokat, amelyeket ők osztottak meg! Miben különbözik az ilyen megosztás attól, amikor az iskola hálózatán másoljuk mindenki által elérhető helyre a fájljainkat?

Hatékony és etikus kommunikáció az interneten

Kérdések

1. Melyek az online csevegés, a chat általunk használt legfontosabb szinterei?
2. Ugyanott csevegünk a szüleinkkel és az osztálytársainkkal, barátainkkal?
3. Csevegünk-e a nagyszüleinkkel?
4. Milyen alkalmazásokat használunk csevegésre?
5. Inkább telefonon vagy inkább számítógépen csevegünk? Miért? Mik az előnyei, és mik a hátrányai az egyiknek és a másiknak?
6. Ha már úgyis csevegünk, akár videótelefonálhatnánk is. Vagy nem? Mikor melyiket használjuk?
7. Mik a csevegés előnyei a hanghívásokhoz képest? És mik a hátrányai?
8. Mi a különbség a chat és az SMS között?

Csevej

A **chatelés** kezdetei a múlt évezredre nyúlnak vissza. Ekkor még külön programmal csatlakoztunk kifejezetten olyan szerverszámítógépekhez – webes szolgáltatásokhoz –, amelyeket üzemeltetőik azért tartottak fenn, hogy az úgynevezett IRC- (Internet Relay Chat) programokkal cseveghezzünk egymással. Ahogy a weboldalak lassan webes alkalmazásokká alakultak, megjelentek a böngészőprogramban is használható csevegőfelületek. Ez azért volt fontos, mert böngészőt használni sokkal többen tudtak, mint ahányan az IRC-vel boldogultak. Az okostelefonok és a bárhol elérhető internet elterjedésével az online chat gyakorlatilag általánossá vált.

A csevegés számos karakter beírásával jár, ami sok idő. Részben ez az oka, hogy a szavak elkerülésének több formája is kialakult.



- Hány üzenetet kapunk naponta? És vajon hány fontosat?

Kérdések

1. Mik azok az emoji-k? Tudjuk-e, hogy milyen jeleket váltott fel a használatuk?
2. Ismerünk-e olyan „szavakat”, rövidítéseket, amelyeket a rendes írott nyelvben nem, de a csevegésben előszeretettel használunk?
3. Hallottunk-e már olyat, amikor valaki egy-egy helyzetben azt mondja: „Hát ez LOL”? Mit jelent a „LOL” kifejezés, honnan ered? Látunk-e problémát abban, ha valaki az említett módon fogalmaz személyes beszélgetések alkalmával?
4. Vannak, akik szerint az emotikonok használata azoknak való, akik végképp nem tudják rendes szavakkal kifejezni magukat. Mi a véleményünk erről a megállapításról?

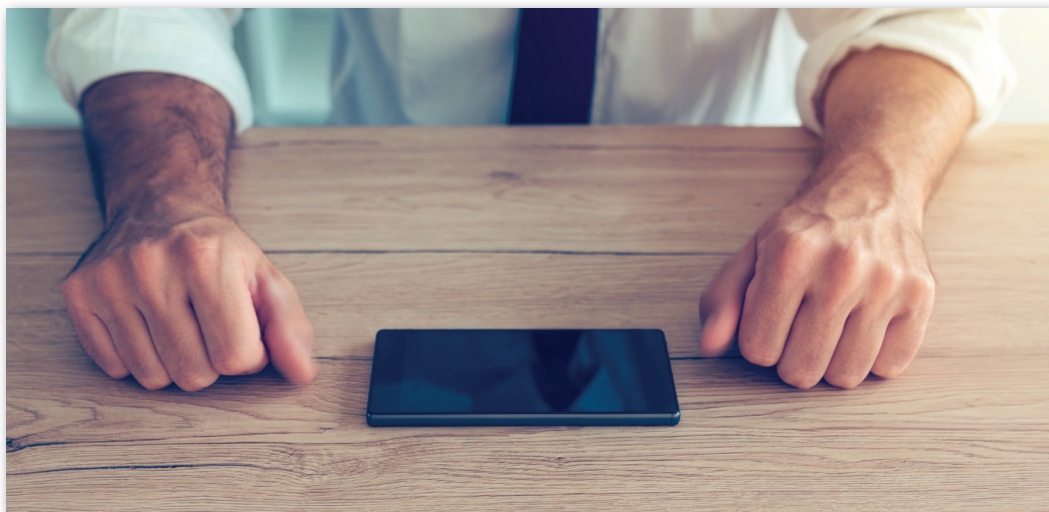
A chatelést lehetővé tevő alkalmazások üzemeltetése nem olcsó dolog. Az üzemeltető cégnek ki kell fizetnie többek között azokat a számítógépeket, amelyeken ezek a szoftverek futnak a felhőben, illetve a fejlesztőket, akik a programokat megírják és karbantartják.

Mégis ingyenesen chatelhetünk. Vannak olyan alkalmazások, ahol az ingyenességet azért biztosítják, mert az üzemeltető cég mesterséges intelligenciája „belehallgat” a chatelésbe, és igyekszik az érdeklődésünknek jobban megfelelő reklámokat eljuttatni hozzánk. Más esetben az üzemeltető cég abban bíz, hogy váltani fogunk a szolgáltatás fizetős, kibővített lehetőségeket kínáló változatára. Van olyan alkalmazás is, amelyet nem üzleti alapon üzemeltetnek, azaz nem cél a pénzkeresés, mert a cég adományokból tartja fenn magát.

Kérdések

1. Hány órát várja naponta a telefonunk az üzeneteket? Hány üzenetet kapunk egy nap alatt? Mennyi ezek közül az igazán fontos? Általában mennyi idő telik el két üzenet fogadása között, amikor be van kapcsolva a telefonunk? Hányra válaszolunk?
2. A nap melyik időszakában jön a legtöbb üzenet?
3. Miért jelenik meg valamilyen jelzés, amikor a beszélgetőpartnerünk épp szöveget ír be?

Vannak olyan mérések, amelyek szerint, ha elmélyült tevékenységet végzünk – például tanulunk –, és a tevékenységből kizökkent valami – például a telefon jelzése az új üzenetről –, akkor húsz percbe is beletelhet, mire ismét teljesen a feladatunkra tudunk koncentrálni. A megállapítást továbbgondolva: ha egy órát tanulunk otthon, és közben háromszor megnézzük a telefonunkat, akkor alig volt értelme leülni tanulni. Más vizsgálatok szerint sokak esetében nem elég, ha lenémítják és lefordítják a telefonjukat, mert ilyenkor egyfolytában azon jár az eszük, hogy jött-e üzenet. Nekik meg kell tanulniuk elfelejtkezni a telefonjukról – amit nagyon megnehezít a kialakult vagy kialakulóban lévő függőség.



► Te használsz a telefonodat, vagy a telefonod használ téged?

Levelezés

Az **e-mail** gyökerei a chateléshez hasonlóan a múlt évezredre nyúlnak vissza. Sokáig egyeduralkodó internetes kommunikációs forma volt, később pedig sokan gondolták, hogy a chatelés elterjedésével eltűnik majd. Napjainkra mindkettőnek meglett a maga szerepe. Bár az e-mailt az iskolások nem igazán használják, a felnőtt életben nagyon fontos a szerepe.

Kérdések, feladatok

1. Van e-mail-címünk? Mennyire gyakran használjuk?
2. Kapnak-e a szüleink e-maileket? És szoktak-e írni?
3. Gyűjtsünk össze olyan eseteket, amikor nem szokás chatet használni, hanem e-mailben írjuk meg a mondandót!
4. A chat vagy az e-mail alkalmasabb-e a hosszabb gondolatok kifejtésére?
5. Chatben vagy e-mailben könnyebb-e visszakeresni egy információt (például, hogy hánykor és hol találkozik az osztály kirándulás előtt)?
6. Hogyan tudunk internetes hivatkozást elküldeni? Küldjünk e-mailt vagy üzenetet kedvenc videónk, online hallgatható zeneszámunk vagy egy jól sikerült kép hivatkozásával!
7. E-mailben vagy chatben küldjük-e el szívesebben a pár pillanattal ezelőtt készült fotót? Miért?

Az e-mailek írásakor biztosan kitöltjük a **Címzett** (angolul: To) mezőt. Nagyon fontos volna kitölteni a **Tárgy** (angolul: Subject) mezőt is, de a gyakorlatlan e-mailezők erről rendszerint megfeledkeznek. Így ha valaki reggel a számítógépét megnyitva sok-sok levelet talál az elektronikus postaládájában, nehezen tudja eldönteni, hogy melyiket fontos azonnal elolvasnia, és melyik ér még rá később.

A **Másolat** (az angol carbon copy, azaz fénymásolat kifejezést rövidítve: Cc) mezőt általában akkor használjuk, ha az elsődleges megszólított mellett további címzetteket szeretnénk becsatolni a levélbe. Ezeknek az e-mail-címeknek a tulajdonosai ugyan megkapják a levelet, de tudják, hogy elsősorban nem nekik szól, hanem csak a feladó szerette volna, ha ők is látják. Ha például levelet írunk az osztályfőnökünknek, elmagyarázva, hogy miért szakadt le a fogas, és a szüleinknek is küldünk másolatot, akkor ők is látják, hogy mennyire felnőtt módon intézzük az ügyeinket, de nem lepődnek meg, hogy miért hívjuk őket Irma néninek. Ha egy cégben a beosztott megírja azt az alkatrész-megrendelést, amit a főnökkel előtte leegyeztetett, akkor a levelét az alkatrészt forgalmazó cégnek címezi, de a főnöknek is küldhet másolatot. A főnök így tudja, hogy a megrendelés rendben ki lett küldve.

Az e-mailek **Titkos másolat** vagy Vakmásolat (angolul blind carbon copy, Bcc) mezőjébe írt címekre szintén elmegy a levél, de erről csak az szerez tudomást, aki így kapja meg a levelet. Sem a címzett, sem a rendes másolatot kapók, sem a többi vakmásolatot kapó cím tulajdonosa nem látja a Titkos másolat mező címzeit. A Bcc mező használata például olyankor szokásos, ha sok embernek küldenénk el egy levelet, de nem szeretnénk, ha mindenki megtudná a többiek címét. A Címzett mezőt nem hagyhatjuk üresen, de azt semmi nem tiltja, hogy mi magunk legyünk a címzett is, ne csak a feladó. Az igazi címzettek kapnak titkos másolatot.

Az emberek e-mail-címe személyes adat, nem adjuk oda másnak – ahogy például a telefonszámokat sem. A cégek e-mail-címei nem számítanak bizalmas adatnak, fel szokták tüntetni őket a cég honlapján is.

Véleménynyilvánítás

Az interneten megosztott képekhez, videókhoz, cikkekhez kapcsolódóan szokás **hozzászólásokat**, idegen szóval kommenteket írni. A hozzászólók jó esetben udvariasan mondják el véleményüket az adott témáról. Ennek ellenére nagyon gyakori a hétköznapiakra, a személyes kapcsolatokra nem jellemző durva nyelvezet használata, a kioktató és sértő hangnemű megszólalás. Jó érzésű ember a hozzászólásaiban is úgy fogalmaz, mintha a többiek – a videó, a kép, a cikk alkotója és valamennyi hozzászóló – vele egy szobában ülnének.



Kérdések, feladatok

1. Kik azok az internetes trollok? Mit jelent a „széttrollkodni” kifejezés? És mit jelent az, hogy „Ne etesd a trollt!”?
2. Vajon miért durvábbak az emberek a kommentekben, mint a személyes találkozások alkalmával?
3. Mit tegyünk, ha a mi megosztásunkhoz vagy hozzászólásunkhoz érkezik sértő, megalázó hozzászólás? Mennyire kell komolyan vennünk? Kihez fordulhatunk segítségért?
4. Mi szokott történni azokkal, akik túl komolyan, nagyon is a szívükre veszik mások agresszív internetes megnyilvánulásait? Keressünk ilyen esetekről szóló tudósításokat!



► Ne tulajdonítsunk túlzott fontosságot jelentéktelen dolgoknak!

Adatvédelem az interneten

Az interneten sokan és sokféleképp próbálkozhatnak személyes adataink megszerzésével. Mielőtt rátérnénk arra, hogy ennek ugyan mi értelme lehet, nézzük máris e lecke legfontosabb mondanivalóját!

Mindig az legyen a kiindulópontunk, hogy **nem adunk meg másnak személyes adatokat!** Ha valaki a személyes adatainkról érdeklődik, ez legyen az alapvető hozzáállás. Ettől akkor térjünk csak el, vagyis akkor adjunk meg adatot, ha

- nekünk is fontos, hogy a másik ember vagy cég tudja az adatainkat, és
- meg vagyunk győződve arról (akár utánajárás útján), hogy ez a másik ember vagy cég nem tud vagy nem fog visszaélni az adatainkkal!



► Nem mindig lehetünk biztosak benne, hogy ki ül a képernyő túloldalán

Mik is azok a személyes adatok?

Vannak olyan adatok, amelyek bennünket mint személyt azonosítanak (azaz megkülönböztetnek mindenki másától). Ilyen adat

- a nevünk,
- az édesanyánk születési (régábbi kifejezéssel: leánykori) neve,
- a személyi azonosító számunk,
- a születésünk helye és ideje,
- a társadalombiztosítási azonosító jelünk (taj), amelyet elsősorban orvosnál, gyógyszerárban használunk, és
- az adószámunk.

Ezeket az adatainkat a hivatalos életben, például iskolai beiratkozáskor, munkahelyre való belépéskor, lakcímváltozáskor, orvosnál, biztosításkötésnél, bankban vagy épp lakás, autó adásvételekor kötött szerződésekben használjuk. Ilyenkor meg kell adnunk őket. De ha ellenőrizetlen helyen, például egy-egy honlap kérdéseire válaszolva adjuk meg ezeket az adatokat, akkor visszaélhetnek velük, például a honlap számunkra teljesen ismeretlen üzemeltetője esetleg a nevünkben eljárva intézhet ügyeket.

Kérdés

Hogyan lehet visszaélni a fenti adatokkal? Nyugodtan eresszük szabadjára a fantáziánkat, valószínűleg semmi olyan nem fog az eszünkbe jutni, amit ne követtek el már sokszor mások személyes adatainak birtokába jutó, rosszindulatú embertársaink.

Vannak olyan személyes adataink, amelyek segítségével el lehet bennünket érni. Ilyen például

- a lakcímünk (bár ezt sok helyzetben az előző adatcsoport részeként, egy személy azonosítására is használják),
- a telefonszámunk és
- az e-mail-címünk.

Ezeknek a megadása, kiadása általában kisebb veszéllyel jár, de épp ezért sokszor lényegesen zavaróbbak a következményei: kéréses reklámhívások, reklámlevelek. Fontos megjegyeznünk, hogy a lakcímünk törvényesen is megszerezhető az országos hatóságoktól, amíg a címünk kiadását meg nem tiltjuk (lásd www.nyilvantarto.hu).



A kéréses e-mailek előzetes beleegyezés nélküli küldése magánszemélyek e-mail-címére a jog szerint tilos. (Az „előzetes beleegyezés” alatt a gyakorlatban többnyire a hírlevelekre való feliratkozást értjük.) A jogi szabályozásnak köszönhetően az európai cégektől jóval kevesebb kéréses levél jön, mint egy bő évtizeddel ezelőtt – de azért jócskán akad még belőlük. A nevesebb e-mail-szolgáltatók nagy erőfeszítéseket tesznek a kéréses levelek, a levélszemét, azaz a spam kiszűrésére.

Az interneten az e-mail-címünket többnyire weboldalakra való regisztrációk során kell megadnunk, a lakcímet és a telefonszámot pedig webshopokból való rendeléskor kérdezi meg a webshop oldala.

Kérdések

1. Milyen szabály vonatkozik a tizennégy év alattiak és a tizennyolc év alattiak weboldalakra történő regisztrációjára? (Segít a hatodikos könyv.)
2. Miért lehet érdekes egy webshopos szállításkor a telefonszámunk?
3. Jelenthet-e veszélyt, ha rosszindulatú, a lakcímünket ismerő ember elolvassa a honlap kezdődő kéthetes nyaralásunkról szóló lelkendezésünket a közösségi médiában?

Személyes adataink harmadik csoportjába soroljuk azokat az adatokat, amelyekkel az e-mail-fiókunkhoz, illetve a különféle webes szolgáltatásokhoz férünk hozzá. Idetartozik a telefonunk, mobilkészítők, számítógépünk jelszava, PIN-kódja vagy bármilyen olyan adat, amely az említett eszközök, weboldalak, szolgáltatások használatához szükséges.



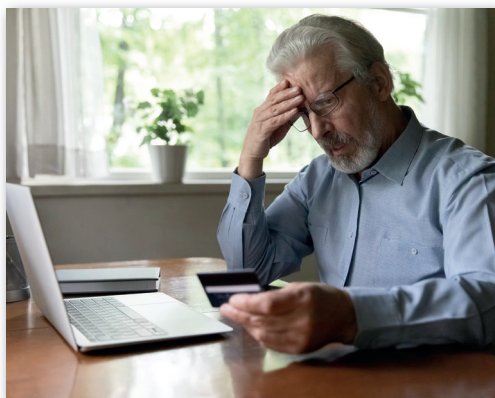
Aki ezek birtokába kerül, az a nevünkben cselekedhet. *Soha nem fordulhat elő*, hogy ezeket bárki, bármilyen weboldal vagy beszállítópartner jó szándékkal kérdezi tőlünk az interneten – és a való életben is csak egészen különleges alkalmakkor. Nagyon-nagyon gondoljuk meg, hogy kiadjuk-e őket!

- Vigyázzunk az eszközeink hozzáférési adataival! (Persze nem kell pont ilyen arckifejezést felvinnünk hozzá.)

Kérdések, feladatok

1. Mi a teendő, ha a közösségi oldalakhoz, webshopokhoz tartozó jelszavunkat elfelejtjük?
2. Mi a teendő, ha a telefonunkhoz tartozó hozzáférési kódokat felejtjük el?
3. Mi a teendő, ha elfelejtjük e-mail-fiókunk jelszavát?
4. Melyik a rosszabb: ha egy webshophoz, egy közösségi oldalhoz vagy az e-mail-fiókunkhoz való hozzáférésünket szerzi meg valaki? Miért?
5. Mit nevezünk kétfaktoros vagy többfaktoros azonosításnak, és hogyan működik? Keresünk róla cikket, videót az interneten!

A személyes adataink utolsó csoportjaként azokat említjük, amelyekkel internetes vásárlások intézhetők. Az internetes vásárlások alkalmával Európában leggyakrabban bankkártyával fizetünk. Sokáig elég volt, ha a bankkártyánkon lévő számokat, illetve a kártyára írt nevet adtuk meg ilyenkor, azaz ha valaki lefényképezte a bankkártyánkat, nyugodtan tudott a nevünkben vásárolni. Ma már általában a bankunkban előzetesen rögzített jelszó megadása, sőt egy vagy több, SMS-ben érkező kód megadása is szükséges az internetes fizetés során.



Kérdések, feladatok

1. Tekinthejtük-e többfaktoros azonosításnak a bankkártyás vásárlásra vonatkozóan említett követelményeket?
2. Mi az a virtuális bankkártya, és hogyan működik? Keresünk róla cikket, videót az interneten!

Alapelv tehát, hogy adatainkra vigyázunk, a saját, immáron egészen jól felfogott érdekünkben. Mások adataival is hasonló felelősséggel kell bánnunk. Nem adjuk meg másnak a barátaink, szüleink, de egyáltalán senkinek az elérhetőségét anélkül, hogy előzőleg az illető hozzájárulását ne kértük volna. Meg sem próbáljuk megtudni, hogy valaki hogyan oldja fel mobil eszközének zárolását, és nem figyelünk árgus szemmel, amikor a padtársunk a jelszavát adja meg. Ha mégis tudomásunkra jut ilyen adat, akkor szóljunk róla!

Adathalászat és egyéb támadások

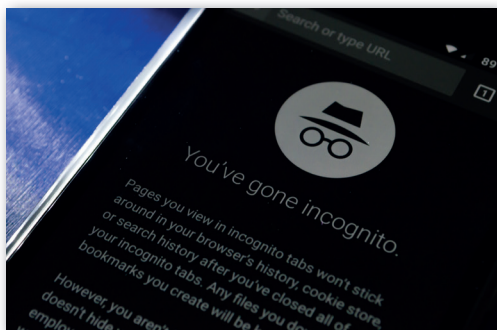
Láttuk, hogy a személyes adatok értéket képviselnek. Megszerzésükre egész internetes „iparág”, az adathalászat (angolul a fishing – halászat – szót szándékosan rosszul írva: phishing) szakosodott, az internetes bűnözés kiterjedt világának részeként. Eszköztáruk rendkívül változatos. Elég hatásosak a megtévesztő e-mailek, amelyekben



- Hogy tudnánk elmondani az adathalászat lényegét a tízéves kistestvérünknek?

banki tisztviselőnek, hivatalnoknak, rég elfeledett rokonnak adja ki magát a levél írója, és így kér adatot.

Gyakran készülnek olyan weboldalak, amelyeknek a kinézete a megtévesztésig hasonlít például egy közösségi oldalhoz, egy bankhoz, de a címe egyetlen betűben eltér az igaziétól. Hányan vesszük észre, hogy a böngésző címsorában nem *azenweboldalam.hu*, hanem *azenwebolbalam.hu* vagy *azenweboldalam.hr* szerepel? Ha egy hibás hivatkozás, egy elgépelés miatt nem a megfelelő weboldalra jutunk, de a kinézete megtéveszt bennünket, és megadjuk a felhasználónevünket és jelszavunkat, akkor már meg is történt a baj, mert a weboldal feljegyezte az adatokat. A nagyobb weboldalak úgy is küzdenek az ilyen kísérletek ellen, hogy az igazi címükhöz nagyon hasonló címeket is lefoglalják. (Ilyet látunk például, ha az egyik híres képmegosztó nevének utolsó betűjét „gépeljük el”.)



► Mire való az inkognitómód a böngészőkben?

Nem szeretjük, ha a weboldalak unostalan jelszót kérnek tőlünk. Ezért aztán a weboldalak a hozzáféréshez szükséges adatokat kis méretű fájlokban elmentetik a böngészőnkkel. Az ilyen fájlok neve süti, angolul cookie. Mód van arra is, hogy a jelszavunkat a böngésző tárolja. A weboldalak használata lényegesen kényelmesebbé válik, de ez azzal jár, hogy aki megszerzi a hozzáférést a számítógépünkhöz, a telefonunkhoz, az hozzáférhet sok internetes fiókunkhoz is.

Kérdések, feladatok

1. Mit tehetünk, hogy az eltűnt, elhagyott, elloptott telefonhoz, laphoz való illetéktelen hozzáférést megnehezítsük, és megkönnyítsük a megtalálásukat? Keressünk praktikákat az interneten!
2. Hogyan lehet megoldani, hogy a böngészőnk egyáltalán ne tároljon sütiket? Hogyan tudjuk törölni az eddig tároltakat? Milyen veszélyekkel jár, ha a böngészőnkben tároljuk a különféle weboldalakon használt jelszavainkat?
3. Hogyan tudjuk a közösségi oldalakon elérhető személyes adatainkhoz való hozzáférést befolyásolni?