

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 mástól). 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: kéréslen reklámhívások, reklámlevelek. Fontos megjegyeznünk, hogy a lakcímünk törvényesen is megszerezhető az országos hatóságoktól, amíg a címünk kiadását meg nem tiltjuk (lásd www.nyilvantarto.hu).



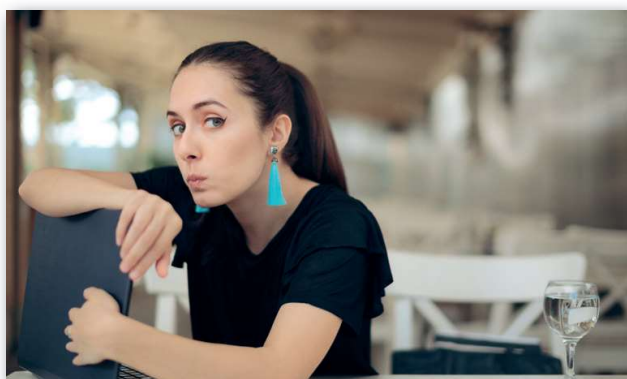
A kéréslen e-mailek előzetes beleegyezés nélküli küldése magánszemélyek e-mail-címére a jog szerint tilos. (Az „előzetes beleegyezés” alatt a gyakorlatban többnyire a hírlevelekre való feliratkozást értjük.) A jogi szabályozásnak köszönhetően az európai cégektől jóval kevesebb kéréslen levél jön, mint egy bő évtizeddel ezelőtt – de azért jócskán akad még belőlük. A nevesebb e-mail-szolgáltatók nagy erőfeszítéseket tesznek a kéréslen 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, mobileszközünk, számítógépünk jelszava, PIN-kódja vagy bármilyen olyan adat, amely az említett eszközök, weboldalak, szolgáltatások használatához szükséges.



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

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

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. Tekinthetjük-e többfaktoros azonosításnak a bankkártyás vásárlásra vonatkozóan említett követelményeket?
2. Mi az a virtuális bankkártya, és hogyan működik? Keressünk 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 mobilkészülékének 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

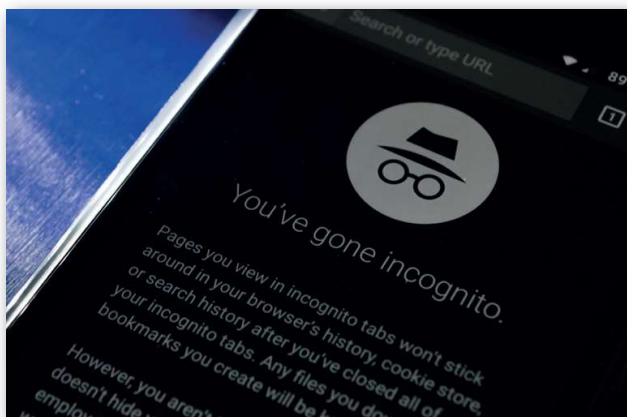
Láttuk, hogy a személyes adatok értéket képviselnek. Megszerzésükre egész internetes „iparág”, az adathalászat (angolul a fishing – halászat – szót szándékosan rosszul írva: phishing) szakosodott, az internetes bűnözés kiterjedt világának részeként. Eszköztáruk rendkívül változatos. Elég hatásosak a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