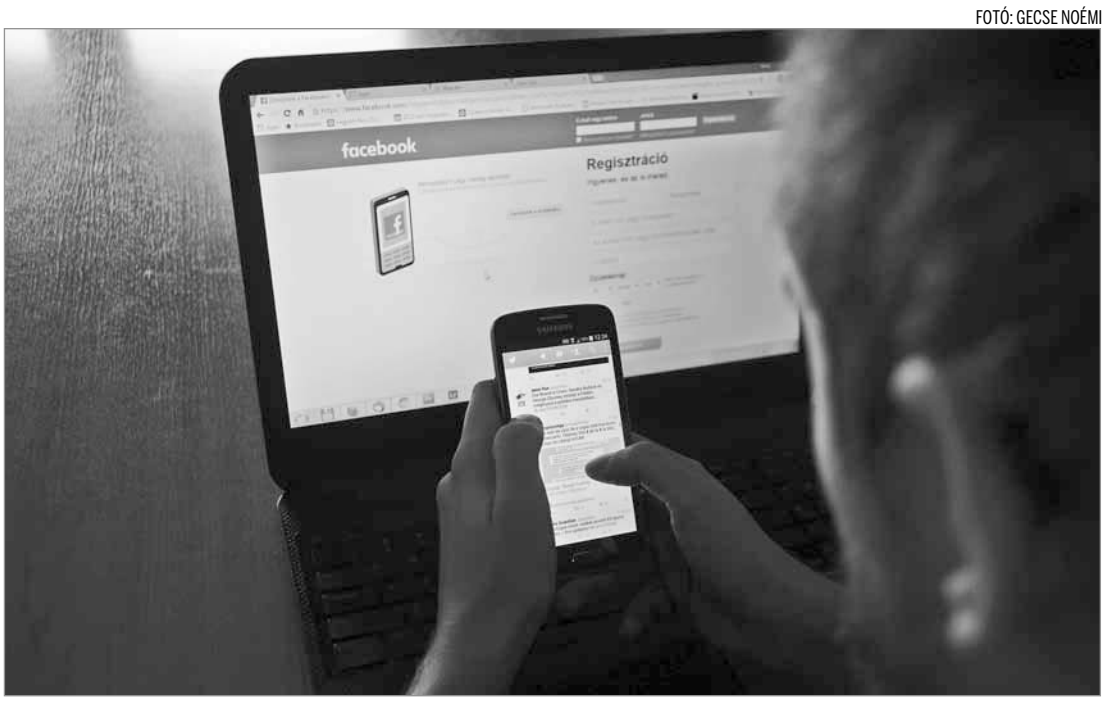
FOLYTATÁS A 6. OLDALRÓL

Ahogy a szenátusi meghallgatáson is többször szóba került: a Facebook üzleti háttere gyakorlatilag átláthatatlan. Mark Zuckerberg elmondta: a szigorítások után nem biztos, hogy a kisebb cégek meg tudják majd fizetni a Facebook-hirdetések árát.

FOTÓ: GECSE NOÉMI



Biztonságos-e a Facebook? A jóhiszeműséget és a megfelelő adatkezelést soha nem vehetjük biztosra

Ha más kezeli adataid, az nem biztonságos

A Facebook-botrányhoz hasonló informatikai visszaélések újra és újra fölvetik a világhálón kommunikálók adatainak biztonságát, amelyek nem csak a legnagyobb közösségi hálón vannak veszélyben. Aki nem elővigyázatos, attól a pillanattól kiszolgáltatottá válik, hogy személyi számítógépe a világhálóra kapcsolódik. Molnár Sándor kolozsvári informatikai szakembert (portrénkon) arról kérdeztük, hogyan csökkenthetjük minimálisra a világhálón való barangolás kockázatait. A szakember szerint van egy aranyszabály: ha adataink feltöltését megtanultuk, megvédésüket is el kell sajátítanunk. Ha nem tesszük, akkor a számítástechnika kiszolgáltatottjaivá váltunk. Ennek felismeréséhez 87 millió felhasználó személyes adatainak illegális elkobzása kellett. Pedig idáig is védtelenek voltunk, csak nem szivárogtak ki hasonló horderejű információk.

„Ha más kezeli az adataidat, akkor sajnos benne van a pakliban, hogy jóváhagyásod nélkül eladhatja azokat" – magyarázza Molnár Sándor a Facebook-botrányra utalva. A szakember szerint más cégeknél is lehetnek hasonló esetek, de ezek még nem derültek ki, vagy soha nem kerülnek nyilvánosságra. A jóhiszeműséget és a megfelelő adatkezelést soha nem vehetjük biztosra.

A bizalmas levelezés tévhite

A nagy internetes vállalatok jelentős hangsúlyt fektetnek a biztonságra. Ez érdeküknek, mivel elsősorban a reklámokból, illetve a látogatottságból élnek. Az adatvédelmi botrányok nagymértékben csökkenthetik hírnevüket, ami komoly veszteséget okozhat számukra. Emiatt nagyon vigyáznak a hírnevükre, azonban baklövések bármikor becsúszhatnak. A Google- és a Yahoo-fiókokat rendkívül sokan használják magánlevelezésre. Nyilvánosan ugyan semmit nem osztanak meg, mégsem lehetnek biztosak abban, hogy a feladón és a címzetten kívül senki nem látja üzeneteiket. A Yahoo-felhasználók adatainak kiszivárogtatása miatt az elmúlt években több botrány is volt.

Fiókunk feltörése esetén az első teendő a jelszó megváltoztatása. Amennyiben az ismeretlen betolakodó már megelőzött ebben bennünket, a helyzetünk kicsit bonyolultabb: ilyenkor a szolgáltatás üzemeltetőjének kell írni, aki – ha elég bizonyítékot kap – visszaadja a fiók fölötti jogunkat, és új jelszót küld.

> A közösségi oldalakon csak azokat a tartalmakat ajánlott megosztani, amelyek idővel sem válhatnak titkossá vagy kellemetlenné.

A közösségi oldalakon csak azokat a tartalmakat ajánlott megosztani, amelyek idővel sem válhatnak titkossá vagy kellemetlenné. A felnőttek ennek határát következetesen megállapíthatják, a kamaszoknak viszont ez nem ilyen egyszerű. Emiatt elengedhetetlen, hogy a szülők felügyeljék a fiatalok internetes tevékenységét, és segítsenek nekik tudatos felhasználókká válni. A törölt tartalmak nem tűnnek el garantáltan a világhálóról, hiszen bárki gond nélkül tárolhatja azokat. „Belső szerverükben a közösségi oldalak feltehetőleg nem raktározzák el a törölt adatokat. Nekik is pénzbe kerül a tárhely, emiatt ha eltávolítottak valamit, előbb-utóbb a szabad hely felülíródik" – közölte a szakember. Megsemmisítése után bizonyos ideig a tartalom visszanyerhető, azonban ez bonyolult művelet, amelyet csak különleges esetekben alkalmaznak, főként nagyvállalatok.

A biztonságos e-mail-kapcsolat maradéktalanul nem oldható meg, azonban bizonyos eszközökkel elősegíthető. „A veszélytelen adatküldéshez külön kódolva kell feltölteni a tartalmakat" – részletezi Molnár. Ingyenes programok segítségével a kódolásokat bárki képes megoldani, ez a művelet viszonylag könnyen elvégezhető. Egyes kódolások szinte maximális biztonságot nyújtanak, hiszen dekódolásuk olyan mértékű energiabefektetést igényel, amely már nem hoz hasznot.

Vírusok a virtuális térben

Személyes adatainkra a számítógépes vírusok is veszélyt jelentenek. Egyik szélsőséges fajtájuk a kémprogram, amely több szinten képes mozogni: ellopja profilunkat, és reklámokkal bombáz, de jelszavakat, illetve bankkártyaadatokat is elcsenhet.

A kémprogramok jelenlétét elsősorban a vírusirtónak kellene észrevennie. A vírusölők önvédelmi mechanizmusát a kémprogramok megpróbálják kikapcsolni, illetve megváltoztatni működésüket. Ha a program nem jelzi a betolakodó jelenlétét, észrevehetjük a számítógép megváltozott működéséből is: lelassul, és feltűnően sokat dolgozik a merevlemez, gyakran lefagy, illetve összeomlik a rendszer. Ilyen esetben a vírusölővel vagy szakértő segítségével szükséges teljes ellenőrzést végezni.

Komoly veszélyt jelentenek azok a programok is, amelyek szerverként használják számítógépeinket: e-maileket küldenek, alkalmazásokat telepítenek, adatokat tárolnak, de akár más gépeket is megtámadhatnak saját eszközünkről. Ezt főként identitásuk elrejtése miatt alkalmazzák nagy sikerrel.

A világhálón fontos a figyelmes jelenlét: meg kell nézni, milyen weboldalakon barangolunk. A nem biztonságos oldalak vírusokat tartalmazhatnak. Emellett a gyanús e-mailek megnyitásakor is ajánlott vigyázni, főként a csatolmányok rejthetnek veszélyeket. Ezekre általában a vírusölők fel vannak készülve, de meghibásodások bármikor történhetnek.

„A vírusirtókról azt kell tudni, hogy egyik sem tökéletes, nem tudnak minden újdonsággal szemben hatékonyak lenni" – magyarázza a szakember. A Windows ezért a rendszerébe saját vírusölőt épített be, de emellett szükséges egy komolyabb programot is telepíteni. Az effajta alkalmazások – bár csökkentik gépünk sebességét, mégis – nagyon hasznosak, mert csökkentik a megfertőződés esélyét is.

Adataink biztonságát a vírusokon kívül az elromlott tárolóeszközök is veszélyeztetik. „Az adatok elveszítésének hangsúlyozása fontos, mert sokan azt képzelik, hogy az adattárolók maximálisan biztonságosak. Ez sajnos nem igaz" – hangsúlyozza Molnár. Fontos tartalmaink megvédése érdekében legalább két vagy három készüléken kell elhelyezni azokat. Például a felhőalapú tárolás megkönnyíti és olcsóbbá teszi a biztonsági mentéseket, valamint a vészhelyreállítás is lehetővé válik.

Figyelhetnek és lehallgathatnak

Leragasztott kamerákat gyakran láthatunk laptoppal rendelkező ismerőseink körében. A jelenség megmosolyogtató, de akár ijesztő is tud lenni, hiszen egy kukkolló az intim tér komoly megsértését jelentené. „Elméletileg lehetséges, de kicsi a valószínűsége annak, hogy valaki a kameránkat használja" – véli Molnár Sándor. A laptopok kamerája rendszerint úgy van megoldva, hogy működésüket kis piros fény jelzi. Ezt ki lehet kapcsolni, azonban nagyon összetett művelet, mivel a meghajtó programban van kódolva.

Az informatikai szakember szerint nagyobb veszélyt jelent a mikrofon bekapcsolása, amely szintén megoldható, és nem látványos. Erre is kicsi az esély, bár a kémprogramok bármire képesek, amit szoftverrel el lehet indítani.

Az online banki ügyintézés során felmerülő kockázatok ezeknél nagyobb veszélyt jelentenek. Előnye, hogy meggyorsítja az ügymenetet, nem kell a tranzakciók miatt személyesen meglátogatni a bankot. Molnár szerint viszont a szolgáltatás komoly veszélyekkel járhat. A bankok különböző technikákat dolgoztak ki, amelyekkel megpróbálják védeni az ügyfelek adatait: kódot küldenek a telefonra, vagy egy hardver eszköz generál kódot. Az sms-ben érkező kód kockázatokkal járhat, amennyiben a telefonon van az alkalmazás is, és az nem rendelkezik komolyabb védelmi rendszerrel: ujjlenyomatolvasóval, arcfelismerővel, íriszleolvasóval vagy komplex kóddal. Ezek főként a drágább telefonok sajátosságai, így az olcsóbb kategóriás mobilokkal rendelkezők nagyobb fenyegetettségnek vannak kitéve. A veszély abban rejlik, hogy maga a banki alkalmazás és a kód is ugyanazon az eszközön található. Tehát ha a telefon rossz kezekbe kerül, a bankszámlát könnyen feltörhetik.

HEVELE LILI, KÁDÁR HANGA

Személyes biztonságunk a Facebookon

Míg egyes közösségi oldalakon – a WhatsAppon vagy az Instagramon például – mindenhonnan törölhetőek az elküldött üzenetek, addig a Facebookon erre nincs lehetőségünk. Ennek ellenére az adatlopás napvilágra kerülése után nem sokkal Zuckerberg – más felsővezetővel együtt – töröltette személyes üzenetváltásait annak ellenére, hogy ezt egy átlagos felhasználó nem teheti meg. A vállalat szerint biztonsági okokból volt erre szükség a CA adatlopása után.

Bár a változtatásokat megígérték, egyelőre még egy vesszőben sem lehetünk biztosak a Facebookon. Választások, népszavazások előtt a legnagyobb segítség, ha nemcsak az üzenőfalon szembejövő cikkekre kattintunk, de tudatosan olvasunk, hallgatunk, nézünk közösségi hálótól függetlenül állami és ellenzéki médiát egyaránt. Ellenőrizzük az alkalmazásoknál a Beállítások menüpont alatt, hogy melyik applikáció, illetve weboldal kaphatja meg adatainkat, illetve ha nem kívánt hirdetést kapunk, a reklám jobb sarkában lenyitható fülre kattintva megnézhetjük a magyarázatot arra vonatkozóan, miért éppen minket ért el az adott hirdetés. Ugyanott jelezhetjük, ha nem érdekel a tartalom. Ahhoz, hogy a Facebook ne személyre szabottan küldjön hirdetéseket, hanem változatosabb tartalmakat kapjunk, valamivel bonyolultabb lépéseket kell tennünk. A Beállítások menüben kiválasztjuk a Hirdetések lehetőséget, utána a Hirdetések a beállított típusaim alapján opciót, majd a Módosításra kattintunk, végül A hirdetéstípusok beállításainak megnyitása lehetőségre. Itt törölhetjük a listából azokat a témákat, amelyekről nem szeretnénk, ha a Facebook további hirdetéseket küldene nekünk.

Azt is beállíthatjuk, mit láthatnak profilunkon azok, akik rákattintnak, de nem ismerőseink. Mindezt az Egyéni adatvédelmi beállításoknál tudjuk elérni képekre és egyéb bejegyzésekre vonatkozóan. Akik egyáltalán nem bíznak a közösségi oldalban, törölni tudják magukat a www.facebook.com/help/delete_account oldalra kattintva. Ez a lépés azonban távolról sem garantálja az internetes lábnyomunk teljes eltűnését.