MALLÁSZ JUDIT

Okos egészségvédelem mobilappokkal

Nem mindegy, hogy melyik mobilalkalmazást használja az ember, legyen szó az élet bármely területéről. Különösen fontos az óvatosság az egészségügyi appoknál.

Mára általánossá vált, hogy számos élethelyzetben mobilalkalmazásokat használunk. Az egyik legnépszerűbb, és sok esetben rendkívül hasznos terület az egészségügy. Se szeri, se száma az appoknak, amelyek – többek között – figyelmeztetnek a mozgásra, monitorozzák napi tevékenységünket és szokásainkat, vagy jelzést küldenek, amikor elérkezett a gyógyszer bevételének ideje. Az appok használatakor azonban gyakran érzékeny adatokat osztunk meg a rendszerrel. A GDPR az egészségügyi információkat „különleges kategóriájú" adatoknak minősíti, ami azt jelenti, hogy nyilvánosságra kerülve „jelentős kockázatot jelenthetnek az egyén alapvető jogaira és szabadságára nézve". Noha a szabályozó hatóságok extra védelemre kötelezik az alkalmazások üzemeltetőit, jó, ha a felhasználók maguk is óvatosak, hiszen nem minden app működik a szabályoknak megfelelően.

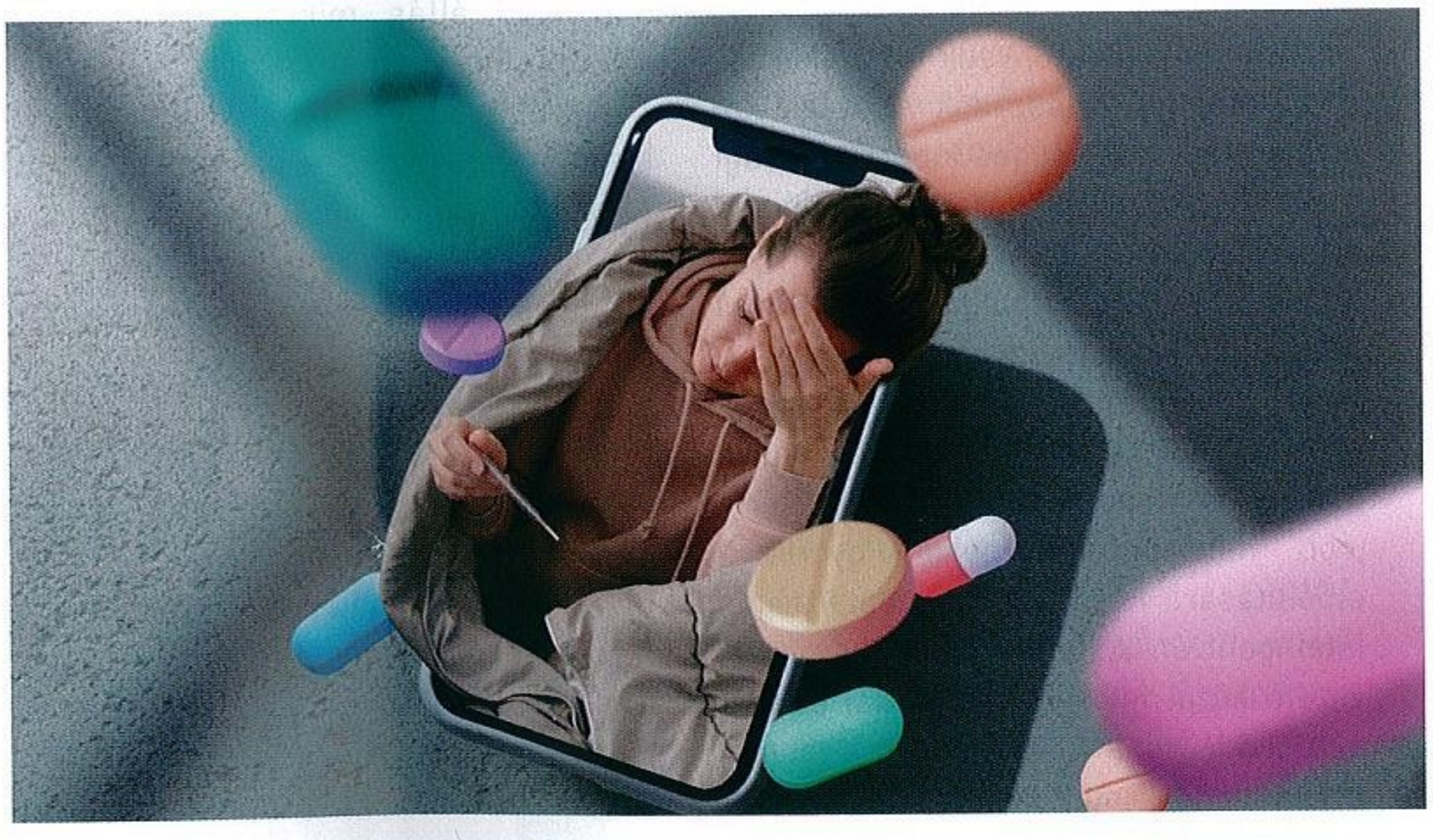
Telepítés előtti tennivalók

– Amikor valaki le akar tölteni a mobileszközére egy alkalmazást, az egyik legfontosabb szempont, hogy megbízható gyártó termékét válassza. Legyen szó bármilyen appról, szinte ökölszabály, hogy a noname, elérhetőséggel nem rendelkező, túl olcsó termékeknél sérülnek vagy hiányosak a kiberbiztonsági előírások. Zárójelben jegyzem meg, hogy ugyanez a helyzet az okoseszközöknél is. Visszatérve az appokra, nem szabad megfeledkezni róla, hogy bármilyen appal hozzáférést adunk telefonunkhoz, amin jellemzően személyes, pénzügyi és egyéb fontos adatok is vannak. Ha pedig valaki az egészségével kapcsolatos adatokat oszt meg, azok esetleges kiszivárogtatása különös, emelt szintű kockázatot jelent – hívja fel a figyelmet *Csizmazia-Darab István*, az ESET megoldásait forgalmazó Sicontact Kft. kiberbiztonsági szakértője.

Előzetes tájékozódáskor hasznos információk nyerhetők ki a felhasználói visszajelzésekből, értékelésekből is. Megnyugtató lehet, ha az app üzemeltetőjének van hivatalos weboldala, az ügyfélszolgálat elérhetőségével, valamint adatvédelmi nyilatkozattal, amely arra is kitér, hogy mit kezdenek a felhasználói adatokkal, hova továbbítják azokat. Jó, ha az alkalmazás független szervezetek által végzett teszteken hosszútávú, stabil, jó eredményeket ért el. Technikai minimumnak tekinthető, hogy az app alkalmazzon titkosítást, tehát a név-jelszó páros ne a sima szövegben utazzon.

fiókokkal, továbbá nem bölcs dolog a bejelentkezéshez a közösségi média fiókot használni. Veszélyeket rejthet magában, ha valaki engedélyt ad az appnak, hogy hozzáférjen a készülék kamerájához vagy a helymeghatározáshoz. Célszerű a hirdetések nyomon követésének korlátozása a telefon adatvédelmi beállításaiban.

– Adnék még néhány általános tanácsot. Az Android-alapú eszközökön mindenképpen legyen vírusvédelem, nem elég, ha rendszeresen érkezik az okoseszközre gyártói hibajavító frissítés, továbbá javasolt egyedi, erős jelszavak használata, kétfaktoros hitelesítéssel.



Nagyon fontos, hogy a profilok legyenek módosíthatóak, törölhetőek. A GDPR előírja, hogy minden cégnek, amelyik európai ügyfeleket szolgál ki, biztosítania kell az adatok törléséhez való jogot, valamint be kell tartania az adatok minimalizálásának elvét. Elgondolkoztató lehet, ha a cég túl friss, csak a közelmúltban alapították. Nyilván jobban meg lehet bízni egy több éves múlttal rendelkező vállalkozásban, mint egy kezdőben. Az is gyanút kelthet, ha nem a témához kapcsolódó adatokat kér az app a felhasználótól. Az alkalmazásokat nem ajánlott összekötni a közösségi

Bármilyen típusú alkalmazást ajánlott a hivatalos piactér alkalmazásboltból letölteni. Természetesen ez sem jelent 100 százalékos biztonságot, de ezeken a helyeken rendszeres az ellenőrzés. A vírusirtó azonban ilyenkor sem felesleges, hiszen az app bármilyen frissítéskor ki lehet téve rosszindulatú támadásnak – figyelmeztet Csizmazia-Darab István.

Szívműtétem volt? Nem is tudtam!

Az illegális úton megszerzett egészségügyi adatok sorsát nem ismerjük annyira, mint például azt, hogy mi a

támadók célja a banki adatok ellopásával. Nyilván eladhatják az adatokat olyan cégeknek, amelyek különféle szempontok alapján adatbázisokat építenek, majd célzott hirdetésekkel bombázzák az érintetteket. Az azonban látszik, hogy a feketepiacon az egészségügyi adatok legalább olyan értékesek, mint a banki adatok.

Ijesztő, hogy az áldozatok általában jó ideig észre sem veszik, hogy ellopták az adataikat, miközben súlyos anyagi károkat szenvedhetnek. Már 2015-ben átlagosan 3,7 millió forintnak megfelelő kárt okoztak a csalók a károsultak nevében megvásárolt, illetve a hamis személyazonosság révén igénybe vett egészségügyi szolgáltatásokkal. Mire egy egészségügyi adattal kapcsolatos lopást, vagy visszaélést a rendszerben észlelnek, jellemzően több mint 3 hónap is eltelhet. Aki ilyen adatlopás áldozatává válik, az átlagosan 200 óra utánajárást, és ügyintézést kénytelen a helyzet tisztázására áldozni, hogy megpróbálja bebizonyítani, nem is ő vette igénybe ezeket a kezeléseket, hanem bűncselekményt történt. – Előfordult például, hogy egy károsult onnan szerzett tudomást egészségügyi adatainak ellopásáról, hogy végrehajtók jelentek meg nála. Kiderült, hogy eltulajdonított adatait felhasználva állítólag szívműtétet hajtottak végre, nagy értékű mozgássérült robogót és több drága orvosi felszerelést vásároltak a nevében. Összességében több tízezer dollárnyi tartozást halmoztak így fel – tájékoztat a Sicontact szakértője.

Az első sorozatos adatlopások óta már majdnem tíz év telt el. Azóta több országban, például Nagy-Britanniában és az Egyesült Államokban külön ügyvédi irodák alakultak, amelyek kifejezetten az ellopott egészségügyi adatokkal kapcsolatos ügyekre szakosodtak, és akár csoportos keresetekben is a fogyasztók érdekeit védik, képviselik kiszivárogtatott személyes, pénzügyi, illetve orvosi és biometrikus adatok esetében.

Néhány évvel ezelőtt a litván Beauty Surgery nevű, kozmetikai műtéteket végző sebészeti klinikán történt egy támadás, amelynek során az elkövetők a személyes adatokon felül mintegy 25 ezer fotót is zsákmányoltak. Ez utóbbiak között sok meztelen, a páciensekről a műtétek előkészítésénél készült fénykép is szerepelt, amelyeket az APT28 támadói csoport fel is töltött a publikus netre. A klinikának kiterjedt nemzetközi ügyfélköre volt, mintegy 60 országból, köztük számos európai országból.

Csizmazia-Darab István elmondta, hogy arra vonatkozó adatok nem vagy csak nagyon hiányosan állnak rendelkezésre, hogy Magyarországon hány olyan incidens történt, amely mobilappok vagy különféle kórházi adatbázisok feltörése révén érte a felhasználókat, illetve milyen jellegű károkozások történtek. Ebből kifolyólag arról sincsenek statisztikák, hogy az egészségügyi alkalmazások milyen mértékű, milyen típusú károkat okoztak használóiknak.

Pénzbírság igen, betiltás nem

Ha kiderül, hogy egy egészségügyi vagy bármilyen más mobilapp használatakor az érzékeny, személyes adatok illetéktelenek kezébe kerültek, a legtöbb ember nyilván megpróbál lépéseket tenni. Hova lehet ilyenkor fordulni?

– Ha közismert szolgáltatóról van szó, a honlapjáról általában kiderül, hogy hova kell fordulni. Adott esetben a hatóságok is lépéseket tehetnek, noha volt már rá példa, hogy egy vírus vagy kémprogram hátterében egy idegen állam állt. Úgy vélem, hogy a külföldről érkező támadások ellen meg kellene védeni a magyar felhasználókat, de mindenkinek magának is ki kell vennie a részét a védekezésben – fogalmaz a kiberbiztonsági szakértő.

Jogos felvetés, hogy amennyiben a károkozás, a személyes adatok illetéktelen eltulajdonítása és felhasználása bebizonyosodik, valahogy szankcionálni kell az elkövetőket. Kézenfekvő a pénzbírság, a kár megtérítése, de adott esetben akár az alkalmazás betiltása is szóba jöhet. – Olyan konkrét esetet nem ismerek, amikor a GDPR-ra hivatkozva betiltottak volna egy egészségügyi alkalmazást. Előfordultak már a GDPR alapján kiszabott pénzbírságok, amelyek közül a legnagyobbakat jellemzően multinacionális vállalatok kapták. Írországban például a Metára 1,2 milliárd euró pénzbírságot szabtak ki az európai felhasználók személyes adatainak megfelelő adatvédelmi mechanizmusok nélkül történő továbbítása miatt. Luxemburgban az Amazonnak 746 milliárd euró pénzbírságot kellett fizetnie, mivel megfelelő hozzájárulás nélkül használta fel az ügyfelek személyes adatait reklámozási célból. Ha személyes adatok szivárognak ki, az sok esetben pénzügyi és egészségügyi adatokat is érint – hívja fel a figyelmet Csizmazia-Darab István. CT