**Tényleg ingyenes? – A mobilappok rejtett kockázataira figyelmeztet a GVH**

*A GVH segít, hogy elkerülje a kockázatos okostelefon-alkalmazásokat*

**Budapest, 2025. augusztus 8. - A mai modern, digitális világban a mobilalkalmazások nélkülözhetetlenek a legtöbb ember életében. Egy mobilapplikáció letöltése előtt azonban érdemes több szempontot is figyelembe venni (biztonság, megbízhatóság, hasznosság). A GVH most tájékoztató anyagokkal segíti a fogyasztókat, hogy megismerjék a mobilapplikációk láthatatlan veszélyeit.**

A digitális világban az okostelefonok és az alkalmazások (applikációk, appok) mindennapi életünk szerves részévé váltak. A vásárlásokon túl használjuk a közösségi kapcsolatteremtéshez, a szórakozáshoz, a tájékozódáshoz, a munkához, az információszerzéshez, a különböző szolgáltatások (pl. közüzemi szolgáltatás, taxi) igénybevételéhez. Az alkalmazásboltok segítségével könnyedén hozzáférhetünk különböző applikációkhoz, amelyek megkönnyítik és színesítik életünket. Azonban nem árt óvatosnak lenni a letöltések előtt, mivel előfordulhat, hogy az ingyenes app később fizetési kötelezettséggel jár, vagy éppen a személyes adatainkra jelenthetnek veszélyt egyes alkalmazások.

**Mire érdemes figyelni az app letöltése előtt?**

* Ismert alkalmazásboltból (App Store, Google Play) töltsön le applikációkat és mindig olvassa el a fogyasztói véleményeket! Az ismeretlen forrásból letöltött alkalmazások kockázatot jelenthetnek.
* Csak az alkalmazás működéséhez szükséges engedélyeket fogadja el! Nézze át a telepítés megkezdése előtt, hogy az applikáció mely más funkciókhoz/alkalmazásokhoz kíván a későbbiekben hozzáférni (pl. névjegyekhez, fotókhoz, kamerához, vagy akár az eszköz helyadataihoz). Amennyiben egy alkalmazás feltételeivel nem ért egyet vagy nem érti, semmiképp se telepítse azt.
* Olvassa el az alkalmazás adatvédelmi szabályzatát! Az adatvédelmi szabályzatból kiderül, hogy az alkalmazás megosztja-e mással az Ön adatait, és ha igen, hogyan, milyen terjedelemben. Homályos szabályzat vagy túl sok adat kérés esetén érdemes inkább elkerülni a letöltést.
* Tájékozódjon, hogy az alkalmazás valóban ingyenes-e vagy esetleg felmerülhetnek később költségek az applikáció használatával!
* Mindig használjon erős és egyedi jelszavakat, amennyiben az alkalmazások regisztrációt írnak elő! Ne használja ugyanazt a jelszavát különböző fiókokban és rendszeresen módosítsa belépési kódjait.
* Lehetőség szerint alkalmazza az úgynevezett „kétlépcsős” azonosítást/hitelesítést! A „kétlépcsős” azonosítás lehetővé teszi, hogy a felhasználó nevének, jelszavának megadásán felül csak további adatok megadásával lehessen belépni az alkalmazásba, így védekezhet az applikáció feltörése ellen.

**Mire figyeljen a már letöltött applikációknál?**

* Nézze át az egyes alkalmazásainak adott engedélyeket! Győződjön meg arról, hogy telepített alkalmazásai csak a valóban szükséges információkhoz férhetnek hozzá, és távolítsa el a szükségtelen engedélyeket. Fordítson különös figyelmet azokra az alkalmazásokra, amelyek hozzáférnek a névjegyzékhez, a kamerához, a tárhelyhez, a képekhez, a helyadatokhoz és a mikrofonhoz. Arra is van lehetősége, hogy egyes engedélyeket csak az alkalmazás használata közben adjon meg. Felülvizsgálhatja az alkalmazás-engedélyeket, beállításokat az [iOS](https://www.apple.com/hu/privacy/control/) és [Android](https://support.google.com/android/answer/9431959?hl=hu) rendszerű készülékek esetében is.
* Tartsa naprakészen az alkalmazásokat és a készüléke operációs rendszerét! Az elavult szoftverrel rendelkező alkalmazások nagyobb veszélynek vannak kitéve, ezért szükség van az alkalmazások frissítésére. A készülék operációs rendszerének frissítése nem csak az új funkciók, hanem a kulcsfontosságú biztonsági intézkedések/javítások elérése miatt is szükséges. Készüléke biztonsága érdekében fontolja meg az automatikus frissítések engedélyezésének lehetőségét, amellyel naprakészen tudja tartani készülékét!
* Törölje azokat az alkalmazásokat, amelyeket nem használ, így csökkentheti az adatgyűjtés kockázatát!
* Legyen óvatos, amikor közösségi fiókokkal (pl. Facebook, Google fiók) jelentkezik be egyes alkalmazásokba! Előfordulhat, hogy az alkalmazás integrálva van a közösségi oldalakkal, ilyen esetben pedig információkat gyűjthet az Ön közösségi fiókjából. Biztonságosabb, ha az alkalmazásokba való belépéshez az e-mail címét használja és egyedi jelszót ad meg!

**Milyen egyéb biztonsági intézkedésekre figyeljen?**

* Ne hagyja felügyelet nélkül a készüléket, mert illetéktelenek hozzáférhetnek az adatokhoz vagy kárt tehetnek bennük!
* Ismerje meg hogyan zárolhatja készülékét vagy törölheti személyes adatait akkor is, ha fizikailag nem fér hozzá készülékéhez! Az Apple Find My iPhone és Android Find My Device olyan helymeghatározó alkalmazások, amelyek egy másik készülék segítségével képesek beazonosítani a saját készülékének helyadatait, ezen felül pedig készülékének zárolására, adatainak törlésére is alkalmasak.
* Állítson be biometrikus azonosítást (pl. ujjlenyomat olvasás, vagy arcfelismerés), így csak Ön férhet hozzá a készülékéhez. Abban az esetben, ha ellopják a mobilját, azonnal lépjen kapcsolatba a szolgáltatójával az adatainak és egyéb értékeinek a védelme érdekében!
* Gyanús üzeneteket ne nyisson meg, és soha ne kattintson az abban szereplő linkekre! Ezek adathalász vagy kártékony tartalmakat rejthetnek.

A GVH azt javasolja, hogy a fogyasztók használják a technika fejlődésével újonnan rendelkezésre álló eszközöket, azonban mindig tartsák szem előtt, hogy a fogyasztó legnagyobb fegyvere és védőeszköze nem más, mint a megfelelő és körültekintő tájékozódás.

A GVH honlapjának [Gondolja Végig Higgadtan](https://www.gvh.hu/fogyasztoknak/gondolja_vegig_higgadtan/7433_hu_gondolja_vegig_higgadtan) menüpontja alatt további hasznos információkat olvashatnak a mobilapplikációkkal kapcsolatban.

**GVH Közszolgálati kommunikációs Iroda**

További információ:

Horváth Bálint, kommunikációs vezető +36 20 238 6939

Gondolovics Katalin, sajtószóvivő +36 30 603 1170