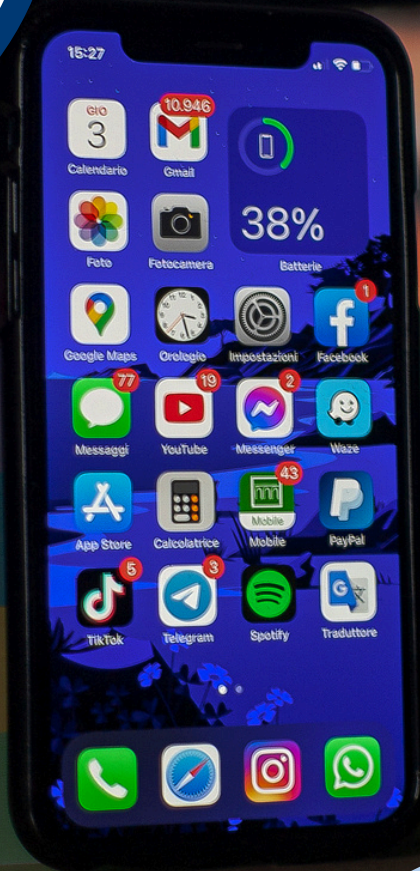


BIZTONSÁGOSAN ÉS TUDATOSAN HASZNÁLJA A MOBILALKALMAZÁSAIT?

 Gondolja
Végig
Higgadtan



GAZDASÁGI
VERSENYHIVATAL



MIK AZOK A MOBIL APPLIKÁCIÓK?

A mai modern, digitális világban a mobil alkalmazások (vagy applikációk, appok) nélkülözhetetlenek a legtöbb ember életében. A fogyasztók a vásárlásokon túl a közösségi kapcsolatteremtéshez, a szórakozáshoz, a tájékozódáshoz, a munkához, az információszerzéshez, a különböző szolgáltatások igénybevételéhez is nap mint nap használnak applikációkat.



A MOBILAPPLIKÁCIÓ vagy **MOBILALKALMAZÁS** okostelefonokra, táblagépekre vagy más hordozható eszközökre fejlesztett, letölthető szoftverprogram, amely valamilyen konkrét funkciót vagy szolgáltatást nyújt a felhasználónak.

A mobilapp tehát egy zsebben hordozható "segítőtárs", ami az okoseszközön különféle feladatokat végez el, a szórakozástól a mindennapi ügyintézésig.



HOGYAN MŰKÖDNEK AZ APPLIKÁCIÓK?

1



LETÖLTÉS ALKALMAZÁSBOLTÓL

Az applikációkat hivatalos alkalmazásboltokból – például App Store vagy Google Play – érdemes letölteni. Mindig megbízható forrásból válasszon!

2



TELEPÍTÉS

A letöltött alkalmazás a telefonra kerül, és kapcsolatba lép az operációs rendszerrel.

3



ENGEDÉLYEK KÉRÉSE

Az app használat közben hozzáférést kérhet különféle funkciókhoz (pl. helymeghatározás (GPS), kamera, mikrofon, internetkapcsolat, névjegyek). Ezek az engedélyek határozzák meg, mit tud rólunk az alkalmazás.

Fontos tudni: Bár az applikációk megkönnyítik a mindennapokat, kockázatokat is rejthetnek:

- az „ingyenes” appok később fizetőssé válhatnak (**freemium modell**),
- egyes alkalmazások pedig **veszélyt jelenthetnek a személyes adatokra.**





MIRE ÉRDEMES FIGYELNI ALKALMAZÁS LETÖLTÉSE ELŐTT?

Az alkalmazás telepítése előtt érdemes néhány alapvető szempontot átgondolni a digitális biztonság megőrzése érdekében.



MIT ÉRDEMES TENNI?



FORRÁS

Ismert alkalmazásboltból történő letöltés (pl. **App Store, Google Play**).



ENGEDÉLYEK

Csak az alkalmazás működéséhez **szükséges engedélyek elfogadása**.



ADATVÉDELEM

Átlátható adatvédelmi szabályzat alapján **eldönthető, mi történik az adatokkal**.



KÖLTSÉG

Figyelni az **előre jelzett költségeket**, az átlátható fizetési feltételeket.



JELSZAVAK

Erős, **egyedi jelszavak használata**, időnkénti módosítás.



KÉTLÉPCSŐS AZONOSÍTÁS

Ha elérhető, érdemes **bekapcsolni az extra védelemért**.

MIRE KELL FIGYELNI?

Ismeretlen forrásból származó alkalmazások kockázatot jelenthetnek.

Ha a hozzáférés nem indokolt (pl. játék kéri a GPS-t), érdemes elutasítani.

Homályos szabályzat vagy túl sok adat kérés esetén érdemes elkerülni inkább a letöltést.

Az „ingyenes” megnevezés mögött rejtett díjak is állhatnak (freemium).

Azonos jelszó több helyen, egyszerű vagy könnyen kitalálható kombinációk.

Bekapcsolás nélkül a hozzáférés könnyebben illetéktelen kézbe kerülhet.



MIT VIZSGÁLJON A MÁR LETÖLTÖTT APPOKNÁL?

ENGEDÉLYEK ELLENŐRZÉSE

Az alkalmazások csak a szükséges adatokhoz férjenek hozzá.

HELYHOZZÁFÉRÉS BEÁLLÍTÁSA

Lehetőség szerint csak használat közben legyen engedélyezve.

A BELÉPÉSI MÓD ÁTGONDOLÁSA

A közösségi fiókos bejelentkezés helyett biztonságosabb lehet az e-mail-es regisztráció.



FRISSÍTÉSEK TELEPÍTÉSE

A legújabb verziók biztonságosabbak, érdemes frissíteni.

A NEM HASZNÁLT APPOK TÖRLÉSE

A felesleges alkalmazások törlésével csökkenthető az adatgyűjtés kockázata.



Gyakorlati útmutatót az alkalmazásengedélyek felülvizsgálatához az **iOS rendszerű** okostelefonhoz [itt](#), az **Android** rendszerű okostelefonhoz pedig [itt](#) érhet el.



EXTRA VÉDELEM: AMIT MÉG ÉRDEMES MEGTENNI

Ahhoz, hogy az adatok és az eszköz is védve legyen, érdemes néhány további óvintézkedést is megfontolni. Ezek segítenek megelőzni az adatlopást, a visszaéléseket és a kellemetlen meglepetéseket – akár készülékhasználat közben, akár váratlan helyzetekben.

A KÉSZÜLÉK FIZIKAI VÉDELME

Ne hagyja felügyelet nélkül a készüléket, mert illetéktelenek hozzáférhetnek az adatokhoz vagy kárt tehetnek bennük.



TÁVOLI ZÁROLÁS ÉS ADATVÉDELEM

Ismerje meg a távoli zárolás és adat-törlés lehetőségeit (pl. Apple Find My iPhone, Android Find My Device). Ezek segíthetnek lopás esetén.

BIOMETRIKUS AZONOSÍTÁS BEÁLLÍTÁSA

Ujjlenyomat vagy arcfelismerés segítségével csak az eszköz tulajdonosa férhet hozzá. Lopás esetén érdemes a szolgáltatót is értesíteni.



ADATHALÁSZAT ELLENI VÉDELEM

Gyanús üzeneteket ne nyisson meg, és ne kattintson linkekre. Ezek adathalász vagy kártékony tartalmakat rejthetnek.



FEJLŐDŐ TECHNOLÓGIA, ÁLLANDÓ TUDATOSSÁG

Fontos, hogy az alkalmazások és tartalomszolgáltatások használata előtt a kapcsolódó feltételek és költségek ismertek legyenek – még ha ezek a szolgáltatások szórakozást, kikapcsolódást vagy segítséget is nyújtanak a mindennapokban.



Gondolja
Végig
Higgadtan

A technológia fejlődésével egyre több eszköz válik elérhetővé, de a legfontosabb védelem továbbra is a tudatos és alapos tájékozódás.

**Szkeneljen
a további információkért!**



www.gvh.hu



GAZDASÁGI
VERSENYHIVATAL