**INFORMATIKA BATXI 1**



Orain testua irakurri eta …

#

# **Kontuz ligatzeko aplikazioekin!**

2017(e)ko azaroak 3. [Iruzkina idatzi](http://www.azkuefundazioarenegunkaria.eus/kontuz-ligatzeko-aplikazioekin/#respond)

Uste baino informazio gehiago sareratzen dugu. Gure datu pertsonalak ematen dizkiegu aplikazio ugariri eta horren adibide dira ligatzekoak. Gure burua deskribatzen ari garenez, datu asko ematen ditugu, horrek izan ditzaken ondorioak kontuan izan gabe.

Gure ibilbideak jasotzen dituzte mugikorrek, nondik nora gabiltzan jakitea ahalbidetuz. Lagun eta senideak zeintzuk ditugun ere esan ohi dugu, baina **zenbait aplikaziori oraindik eta informazio gehiago ematen diegu.**

[**Kaspersky**](https://www.kaspersky.es/)**k argitaratutako azken ikerketak dio mota honetako aplikazioak direla hackeatzen errazenak.** Eta horrelakoetan ez daude bakarrik erabiltzailearen datu pertsonalak; askoz ere gauza gehiago aurkitu daitezke, hala nola, **zer motatako pertsonen bila dabilen, nori eman dio “atsegin dut” eta baita informazio karga handia duten mezu pribatuak ere.**

Ikerketa honetan aztertu diren aplikazioak ligatzekoen artean erabilienak dira: [Badoo](https://badoo.com/es/), [Tinder](https://tinder.com/), [Happn](https://www.happn.com/es/), [OkCupid](https://www.okcupid.com/), [WeChat](https://www.wechat.com/es/) eta [Bumble](https://bumble.com/es/), besteak beste. Guzti hauei azterketa bera egin zitzaien, argitaratutako datuen pribatasuna zer nolakoa zen frogatzeko.

**Tinder, Bumble eta Happnek beste sare sozial batzuetan bilatzen dute erabiltzailea, informazio, datu eta argazki gehiago lortzeko asmotan.** Izan ere, pertsona bat pantaila baten bitartez ezagutzeak oztopoak izan ditzake. Hori dela eta, beste pertsonaren informazio asko izanez gero, hobeto irudikatuko dugu nolakoa den. **“Tindstagram”** izena jarri zaio ekintza honi, bi plataformetan arakatzeko aukera ematen baitu.

**Gainontzeko aplikazioetan izena, adina eta argazkiak bakarrik ematen dira eta beraz, zailagoa da erabiltzailearen beste sare sozial batzuetako kontuak aurkitzea.**

**Kokapenaren inguruko azterketa ere egin dute Kasperskykoek.** Ezin daiteke inor geolokalizatu, baina ikertzaileak erabiltzaileen puntu zehatza emateko gai izan dira, koordenada faltsuak emanez eta pertsona konkretu baten kokapen errealetik zer distantziatara zeuden kalkulatuz.

Kontu hauez gain, l**igatzeko aplikazioek ez dute datuak enkripatzeko aukerarik.** Gabezia horren ondorioz, kontu errealetara jotzeko aukera dago. **Ikertzaileak** [**Mamba**](https://www.mamba.ru/)**ko erabiltzaile batzuen kontuetara sartu ahal izan ziren eta beraiek balira bezala jokatu.**

Hala ere, desabantaila hauei aurre egin eta **modu seguru batean ligatzeko aukera dago**. Horretarako zenbait gauza izan behar dira kontuan:

* Ez erabili WiFi publikoak
* Ez eman informazio eta datu askorik aplikazioei
* Malwareak antzemateko programa bat erabili

Guzti hau jakinda, lasai ligatu ahalko duzu sarean.

