Frendie Kaverisovelluksen turvallisuus

Frendie Kaverisovelluksen turvallisuutta on tutkittu ja kehitetty hyvin paljon tiedostaen yleisesti riskit joita netissä käytävään kanssakäymiseen liittyy. Aihetta on työstetty Frendie Kaverisovellus-työryhmän, sovelluskehityksestä vastaavan kehitysyrityksen, yksinäisyystyön ammattilaisten ja sovelluksen käyttäjien kanssa. Frendie Kaverisovellus-alustan turvallisuus on auditoitu mm. **Suomen Punaisen Ristin, Barona Oy:n sekä Espoon kaupungin** ulkoisen auditoinnin toimesta. Frendie Kaverisovellus on toteutettu alan parhaita käytäntöjä ja korkeaa tietoturvaa noudattaen.

Tekninen arkkitehtuuri ja käytännöt:

Frendie Kaverisovellus on toteutettu Flutter -tekniikalla, hyödyntäen taustajärjestelmänä Googlen Firebase pilvipalveluita. Käyttäjätunnukset ja tunnistautuminen hyödyntää Firebase autentikaatiota.

Palvelun käyttäjät kirjautuvat sähköposti + salasana yhdistelmällä. Käytetty sähköposti varmennetaan ensimmäisen kirjautumisen yhteydessä. Salasanat tallennetaan Firebasen tietokantaan turvallisesti, eikä niitä ole mahdollista purkaa selkokieliseksi.

Käyttäjädatan, kuten profiilien ja keskustelujen tallennus on toteutettu Google Cloud Firestore -tietokantaan. Firestore skaalautuva NoSQL pilvitietokantapalvelu, joka on suunniteltu erityisesti mobiilisovellusten käyttöön. Sen tietoturvaominaisuuksiin lukeutuu: ● Autentikointi: Firestore integroituu Google Cloud Identity and Access Management (IAM) -palveluun, jonka kautta kehittäjätunnukset valtuutetaan pilvi-instanssin ylläpitoon. Käytännössä instanssin ja datan hallintaan vaaditaan Google tunnukset kahdenkertaisella tunnistautumisella
● HTTPS suojatut yhteydet.
● Server-side encryption. Firestore salaa kaikki levylle tallennettavat tiedot automaattisesti. ● Roolipohjainen pääsyvalvonta: Firestore mahdollistaa pääsynhallinnan käyttäjä- ja roolikohtaisesti. Voit määrittää, kuka voi lukea, kirjoittaa tai muokata tietoja tietokannassasi. Jokainen kirjoitus/lukusuoritus on valvottu ja on oltava valtuutettu Security rules -säännöissä.

Keskustelujen viestien lukeminen (Security rules -sääntö) vaatii:

a) kirjautuneen käyttäjän, sekä
b) käyttäjän täytyy olla tallennettu keskustelun osallistujaksi.
Kaverisovelluksella ei ole muuta julkisessa verkossa olevaa hallintakäyttöliittymää kuin pilvipalvelun instanssin työkalut, eikä Kaverisovellus hae tietoja suojaamattomista lähteistä. Rekisteröityessä käyttäjät sitoutuu noudattamaan palvelun sääntöjä. Sovelluksen sisällä on ilmianto-toiminto loukkaavan sisällön tai sääntörikkomusten ilmoittamiseen ylläpidolle.

Tunnistautuminen

Lähtökohta on, että vahva tunnistautuminen olisi paras suoja sille, ettei kukaan halua esiintyä alustalla jonain toisena henkilönä. Tunnistautumisella ei luonnollisestikaan voida 100% ehkäistä alustan väärinkäyttöä, mutta se luo tarvittavan pelotteen kiinnijäämisen riskistä. Tutkimuksemme mukaan turvallinen käyttöönotto vahvan tunnistautumisen keinoin on kuitenkin noussut itsessään epäilyksiä herättäväksi toimenpiteeksi yhteisöalustallemme kirjautuessa. Lisäksi käyttäjiltä saamamme palautteen perusteella vahvan tunnistautumisen sisällyttäminen sovelluksen sisäänkirjautumiseen nostaa kynnystä ottaa palvelu käyttöön sekä heikentää sovelluksen käyttökokemusta. Frendie Kaverisovellus ei tällä hetkellä hyödynnä käyttäjien varmentamisessa vahvan tunnistautumisen palvelua.

Tunnistetut käyttäjät ja moderointi

Frendie Kaverisovellusta on kehitetty yhdessä luotettavien kumppaneiden kanssa. Frendie Kaverisovellus PRO alustalla on mahdollisuus olla läsnä tunnistettuna käyttäjänä (yrityksen HR, TJ, Psykologi, ym.), jotka voivat olla chat-tyyppisesti organisaation tunnuksin kirjautuneiden käyttäjien käytettävissä. Käyttäjät, jotka tulevat sovellukseen tunnistetulla profiililla, ovat ylläpidon tunnistamia ja vahvistamia organisaation henkilöitä.

Sovelluksen ylläpitoon kuuluu aktiivinen moderointi, joka voi olla jatkuvassa vuorovaikutuksessa sovelluksen käyttäjien sekä tarvittaessa tunnistettujen käyttäjien kanssa. Organisaation tunnistettuna käyttäjänä on mahdollista olla aktiivisesti läsnä Frendie Kaverisovelluksessa ja halutessa huomioida muita omaan organisaatioon kuuluvia sovelluksen käyttäjiä. Aktiivinen läsnäolo auttaa myös tarttumaan

nopeammin mahdolliseen häiriökäytökseen tai nettitrollaamiseen. Yhtenä kehityslinjana voisi olla myös koulutettujen ja ohjattujen vapaaehtoisten sovelluksessa mukanaoloa. Tällä hetkellä tätä ominaisuutta rakennetaan sovelluksen kehittäjien toimesta.

Tietojen jako

Käyttäjä ei voi jakaa Frendie Kaverisovelluksen alustalla mitään tiedostoja, esimerkiksi kuvia. Vapaaehtoinen profiilikuva on ainoa tiedosto, jonka sovellukseen voi lisätä. Sovelluksessa käydyt chat-keskustelut tallentuvat sovelluksen ylläpitäjän tietokantaan. Sovelluksen moderointia tekee suomalainen kehitystiimi suomessa ja sovellukseen tallentuva tieto käsitellään eurooppalaisen GDPR-tietoturvaperiaatteen mukaisesti.

Alustalta saa tarvittaessa teknisesti kaiken tiedon jälkikäteen, ja pystytään etsimään tarvittaessa ip-tietoja käyttäjästä. Sovelluksessa ei käytetä tällä hetkellä tarkan sijaintitiedon tallennusta eikä sovellusta käyttävien laitteiden sijaintitiedot tallennu tietokantaan. Frendie Kaverisovelluksessa on mahdollista ilmaista oma kotipaikkakunta ja se syötetään palveluun vapaaehtoisesti ja manuaalisesti.

Ohjeistus turvalliseen ja kunnioittavaan keskusteluun
Sekä sovelluksessa, että siitä tiedottamisessa ohjeistetaan käyttäjiä turvallisen ja kunnioittavan keskustelun periaatteisiin. Yhteiskunnallisena yrityksenä Frendie Kaverisovellus edistää yhteisöllisyyden ja uusiin ihmisiin tutustumisen aihetta yhdessä alan toimijoiden ja ammattilaisten kanssa. Frendie Kaverisovelluksen tiimiin kuuluu yksinäisyystutkijoita sekä lääkäreitä. Ohjeet on tuotettu yhdessä Kulttuuri-ja uskontofoorumi FOKUS ry:n kanssa, filosofian tohtori **Marja Laineen** johdolla.

Turvallisuusohje päivittyy säännöllisesti.