Anti-Vax Dating App Left Data Unprotected

Article By:

Data Privacy & Cybersecurity Robinson Cole

Unjected, a dating app and the "largest unvaccinated platform" online, apparently left its entire website's back end unsecured. Security researchers, working with Daily Dot reporters, reportedly accessed the site's administrator dashboard, which had been left entirely unsecured and in de-bug mode. As a result, they got incredible access, including the ability to view and modify private account details, edit posts, and access backups without administrator authentication. The potentially-exposed personal information included the full name, birth date, marital status, and email address of 3,500 users, though it's unclear whether anyone besides the researchers exploited the exposure. After being informed of the issues, the company took several days to fix the critical security vulnerability.

The Daily Dot contacted several Unjected users about the issue. The members of the unvaccinated dating community did not appreciate being so exposed and unprotected. An anonymous user quoted by the Daily Dot shared their thoughts on an in-app message board: "I'm trying to be as kind as possible when I say, take the app down now before you end up in the courts and don't release it until you do proper software development testing on it."

Unjected describes itself as "a multi-faceted platform of health conscious, covid-19 unvaccinated humans who believe in medical freedom, freedom of choice, freedom of speech & bodily autonomy" where users can "find love with mRNA free partners." The app also offers a fertility directory, where users advertise their vaccine-free semen, eggs, and breastmilk.

This article was authored by Blair Robinson, non-lawyer intern at Robinson Cole.

Source URL:https://natlawreview.com/article/anti-vax-dating-app-left-data-unprotected