Hacker leaks 40 million user records from popular Wishbone app

By Catalin Cimpanu

Published: 2020-05-20 · Archived: 2026-04-05 21:57:44 UTC

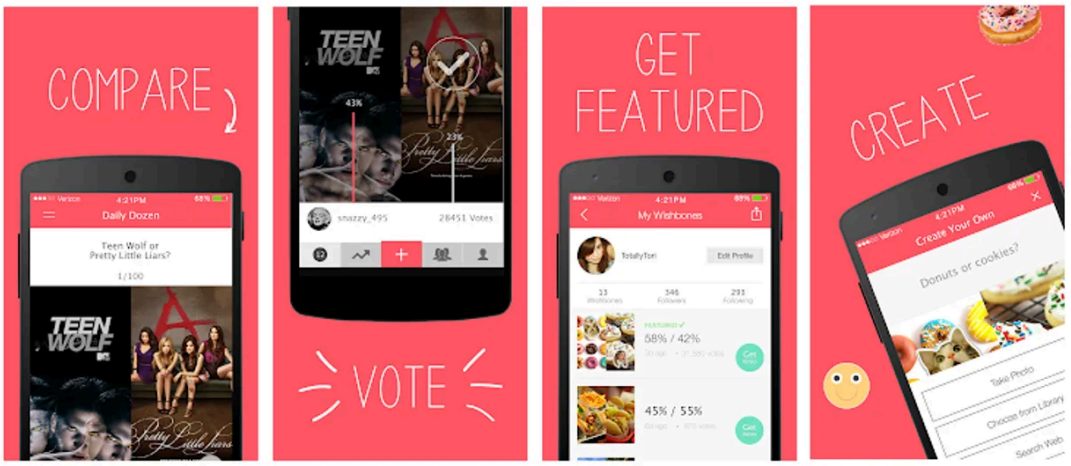


Image via Wishbone website

UPDATE: *Twelve hours after this article went live, the Wishbone user database has leaked in full, being offered as a free download on one of the hacking forums it was being sold on. A well-known hacker known as ShinyHunters has taken credit for hacking the company, and Wishbone has formally acknowledged the breach in a statement sent to ZDNet. Our initial coverage is below, written from the perspective of the database being put up for sale.*

A hacker has put up for sale today the details of 40 million users registered on Wishbone, a popular mobile app that lets users compare two items in a simple voting poll.

The data is being advertised across multiple hacking forums and being sold for 0.85 bitcoin (~$8000), according to ads seen by ZDNet.

According to the seller's claims and a sample of the data published online, the Wishbone data includes user information such as usernames, emails, phone numbers, city/state/country, but also hashed passwords.

wishbone-sample.png
Image: ZDNet

The hacker claims the passwords are in the SHA1 format; however the sample that ZDNet reviewed today contained passwords in MD5.

MD5 is a weak password hashing format that can be cracked to reveal the original plaintext passwords, which ZDNet was able to do for some accounts using freely available online tools.

The data also included links to Wishbone profile pictures. URLs included in the sample data loaded images depicting minors, an age category the Wishbone app has always been historically popular (to many parents' dismay).

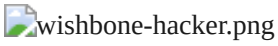
Wishbone hack took place earlier this year

The seller claims the Wishbone app data was obtained in a hack that took place earlier this year. User registration and last login dates included in the Wishbone data sample appear to confirm this statement, with all timestamps dating to January 2020.

It is unclear, however, if the individual who has placed all the ads on hacking forums is the actual hacker.

The person behind the forum ads is what security researchers call a "data broker," a type of cyber-criminal specialized in buying and reselling hacked databases in the cybercriminal underground.

According to ads seen by ZDNet, this threat actor is currently selling databases from tens of other companies, totaling more than 1.5 billion records.



Most of the databases are from companies that have reported hacks in previous years. Wishbone was also hacked in 2017 when a hacker obtained details for 2.2 million users.

ZDNet verified today that the data sample from this recent hack was not included in the 2017 hack. We took user emails from today's data sample and verified them against Have I Been Pwned, a website that lets users check if their emails have been included in previous hacks.

However, since Have I Been Pwned allows users to hide their email from public searches, we also verified these emails against a private platform managed by threat intelligence KELA, which has also been indexing and tracking data leaked in older breaches.

None of the accounts included in the sample shared today were included in the 2017 Wishbone breach, confirming that these are new accounts, and this is a new hack.

Contacted for comment, a Mammoth Media spokesperson told ZDNet they are looking into the matter.

"Protecting data is of the utmost importance," the company said. "We are investigating this matter and will share any significant developments."

While the Wishbone has not revealed in recent years its total user count, the app has been in the iOS App Store Top 50 most popular social networking apps for years, reaching its peak in 2018, when it ranked in the category's top 10. On the Google Play Store, the app has between 5 million and 10 million downloads.
