

Hacker leaks data of millions of Teespring users

By Catalin Cimpanu

Published: 2021-01-21 · Archived: 2026-04-05 23:00:13 UTC



A hacker has leaked the details of millions of users registered on Teespring, a web portal that lets users create and sell custom-printed apparel.

The user data was leaked last Sunday on a public forum dedicated to cybercrime and the sale of stolen databases.

The Teespring data was made available as a 7zip archive that includes two SQL files. The first file contains a list of more than 8.2 million Teespring users' email addresses and the date the email address was last updated.

Also: [Best VPNs](#) • [Best security keys](#) • [Best antivirus](#)


 teespring-emails.png

Image: ZDNet

The second file includes account details for more than 4.6 million users.

Details included in this second SQL file a hashed version of the email address, usernames, real names, phone numbers, home addresses, and Facebook and OpenID identifiers users used to log into their accounts.

Other details related to a user's Teespring online account information is also included and is not believed to be sensitive.

The good news is that not all accounts have this information filled, which reduces how the breach affected each Teespring user to the amount of granular data they provided to the company. Secondly, password data was not included; however, it is unclear if hackers gained access to passwords and just chose not to release them.

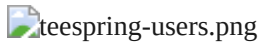


Image: ZDNet

The hacker who leaked the data goes by the name of ShinyHunters, a threat actor that has leaked billions of user records from hundreds of companies.

However, ShinyHunters is not believed to have been the person who breached Teespring.

The company's data was initially offered for sale on the same forum and via private Telegram channels in December 2020, before being leaked for free last week by ShinyHunters in a common practice where data brokers sabotage each others' sales.

A request for comment sent to an email address previously used by ShinyHunters also remained unanswered.

Teespring breach occurred via Waydev app

A Teespring spokesperson told *ZDNet* the company was aware of the breach, which it [disclosed on December 1, 2020](#). The company said the incident took place in June 2020 when a hacker managed to steal user data from its cloud infrastructure.

"Teespring had previously evaluated a 3rd party service called Waydev which required access to some of our data. This access was implemented via a technology called OAuth," the company said.

"Unfortunately, Waydev retained the OAuth token for Teespring (and several other companies) which was accessed from Waydev without authorization by a third party. The token was then used to gain access to some of the Teespring infrastructure."

The [Waydev incident](#) is well known and was previously covered by ZDNet in July 2020.

Teespring, founded in 2011, is currently ranked as one of the most popular 1,500 sites on the internet, on #1,410, according to the Alexa web traffic ranking.

Updated at 12:30pm ET with comment from Teespring.