

Information leak of over 1.2 billion user records stored in an insecure database

International security researchers recently found an unprotected server containing data on 1.2 billion personal records.

International security researchers recently found an unprotected server containing data on 1.2 billion personal records, many of which are thought to have leaked, falling into the hands of organizations. Personally collecting personal data.

This data includes your email address, occupation, location, title, name, phone number and even social media account information.

In late October, two independent security researchers Vinny Troia and Bob Diachenko identified a server called Elasticsearch that contained more than 4 terabytes of data but was almost unprotected. This repository mainly contains information gathered from major social media sources like Facebook and LinkedIn, combined with names, email addresses (both personal and professional), phone numbers, Twitter URLs and Github and many other types of data are commonly used by data brokers (companies specializing in advertising support, marketing and messaging services).

Taken together, these pieces of information provide a relatively detailed view of individuals leaking personal records, even their employment experiences and education levels. All information is not protected, which means anyone can access it easily without having to meet any requirements.

Vinny Troia and Bob Diachenko believe that the insecure database is owned by a large enterprise operating in the field of personal data management called People Data Labs, because the exposed data warehouse contains a Some indicators suggest it originates from this company.



People Data Labs is one of the famous data management support companies in the US and a partner of many big names like eBay, Adidas. The company has not made any comments yet. case.

You finished reading the article "**Information leak of over 1.2 billion user records stored in an insecure database**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.