Data Breach Exposes 6.6 Million PlainText Passwords from Ad Company.

Posted by Hermes 09/15/2016

Another Day, Another Data Breach! And this time, it's worse than any recent data breaches.

Why?

Because the data breach has exposed plaintext passwords, usernames, email addresses, and a large trove of other personal information of more than 6.6 Million ClixSense users.

ClixSense, a website that claims to pay users for viewing advertisements and completing online surveys, is the latest victim to join the list of "**Mega-Breaches**" revealed in recent months, including LinkedIn, MySpace, VK.com, Tumblr, and Dropbox.

Hackers are Selling Plaintext Passwords and Complete Website Source Code

More than 2.2 Million people have already had their personal and sensitive data posted to PasteBin over the weekend. The hackers who dumped the data has put another 4.4 Million accounts up for sale.

In addition to un-hashed passwords and email addresses, the dump database includes first and last names, dates of birth, sex, home addresses, IP addresses, payment histories, and other banking details of Millions of users.

Troy Hunt, operator of Have I Been Pwned? breach notification service, verified the authenticity of the data taken from ClixSense.

Besides giving away 4.4 Million accounts to the highest bidder, the hackers are also offering social security numbers of compromised users, along with the complete source code of the ClixSense website and "70,000 emails" from the company's internal email server, according to a Pastebin message advertising the stolen database.

PasteBin has since removed the post as well as the sample of the compromised database that contained user account information.

Here's How Hackers Hacked ClixSence:

ClixSense admitted the data breach and said some unknown hackers were able to get access to its main database through an old server which the firm was no longer using, but at the time, still networked to its main database server.

After gaining access, the hacker was able "to copy most, if not all" of the ClixSense users table, ran SQL code to change account names to "hacked account," deleted several forum posts, as well as set account balances of users to $0.00.

While talking to Ars Technica, ClixSense owner Jim Grago admitted that the database contained entries for roughly 6.6 Million accounts and that the company became aware of the breach on September 4 and managed to regain control of their DNS over the weekend.

> "This all started last Sunday, September 4th about 5 am EST when my lead developer called me and said ClixSense was redirecting to a gay porn site. The hackers were able to take over our DNS and setup the redirection," Grago wrote.
> "On Monday (Labor day) they were able to hack into our hosting provider and turned off all of our servers, hacked into our Microsoft Exchange server and changed the passwords on all of our email accounts. On Tuesday they were able to gain access to a server that was directly connected to our database server and get a copy of our users table."

Change Your Passwords and Security Questions Now

Users are strongly advised to change their passwords for ClixSence account immediately, and it would also be a good idea to reset passwords for all of your other online services, especially those using the same passwords.

Since ClixSense uses a large trove of personal information on its users, make sure you change your security questions, if it uses any of the information you provided to ClixSense, such as your address, date of birth, or other identifying information.

Moreover, I recommend you to use a good password manager to create strong and complex passwords for your different online accounts, and it will remember all of them on your behalf.

I have listed some of the best password managers that could help you understand the importance of password manager and choose one according to your requirement.
