Not So Smart AI - A Self Inflicted Data Breach at ChatGPT

March 24, 2023 - We've written quite a bit about ChatGPT over the past few months. Yes, it's woke, but it is also very convenient and it delivers information to you without any need to scan through endless ads and numerous pages of information that have nothing to do with what you are looking for. But this past week, it was delivering up information that nobody was looking for. The personally identifiable information of some of its registered users.

ChatGPT can be used for free, but it also has a paid version which currently costs $20 per month. On a side note, why anyone would pay them $20 per month when until just recently it didn't include data later than 2021 is beyond us, but that's another story entirely. They now do have a plugin which allows the service to include more recent data from the internet, so we'd imagine that the number of paid subscribers will begin to increase.

In any case, some users of the service began to notice that chats that they were not a party to had started to show up in their history this past Monday. And in some of those cases, they could see the personal information for the people that had initiated the chat. This information included names, email addresses and the last four digits of the credit cards they used with the service.

OpenAI - the company that owns ChatGPT - has said that the breach was due to a bug in their software and that it affected approximately 1.2% of their paid users. But they haven't said exactly how many paid users they have.

OpenAI has said that they have patched their software to prevent the issue going forward. They have also said that they believe the overall number of people impacted was relatively low.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.