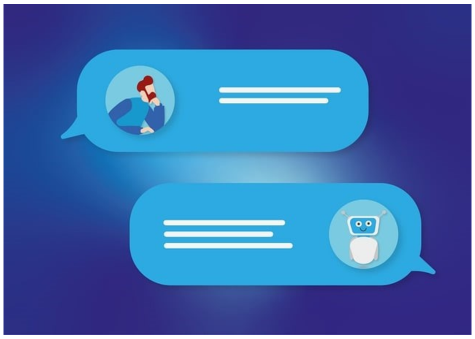
NEWS
CYBER SECURITY
Vol. 9 | Issue 6
June 2024

| Page 2 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter



Generative AI models, like ChatGPT, rely on vast amounts of data to function effectively. When you interact with these models, the data you input can be used to improve the AI's performance.

Here's how this process works:

1. Data Collection: When you input data, it is often collected and stored by the service provider. This data can include text, images, or other forms of input.

2. Training and Improvement: The collected data is used to train and refine the AI model. This helps the AI learn from real-world interactions, enhancing its ability to generate more accurate and relevant responses.

3. Long-Term Storage: In many cases, the data you input is kept indefinitely. This means that any personal or sensitive information you provide could be stored for a long time, *potentially forever*.

Risks of Using Personal Information with Generative AI

- **Data Breach:** If the service provider's database is compromised, your personal information could be exposed.
- **Unauthorized Use:** Your data might be used for purposes beyond what you initially intended, including marketing, research, or even shared with third parties.
- **Privacy Invasion:** Detailed personal information can be pieced together to create a comprehensive profile of you, which might be used for malicious purposes.

Tips to Stay Safe

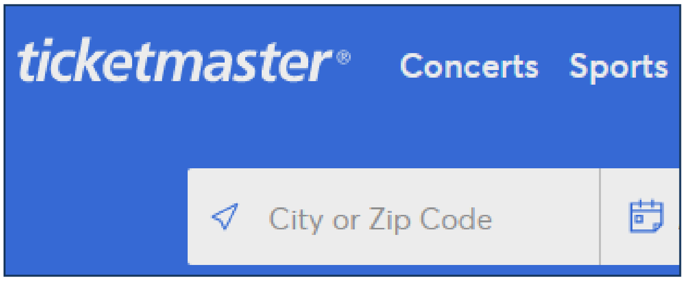
- **Avoid Sharing Personal Information:** Do not input sensitive personal information such as your full name, address, social security number, or financial details.
- **Understand the Privacy Policy:** Before using a generative AI service, read its privacy policy to understand how your data will be used and stored.
- **Use Trusted Services:** Stick to reputable AI services that have robust security measures and transparent data practices.

More on AI and Privacy Concerns: https://www.axios.com/2024/03/14/generative-ai-privacy-problem-chatgpt-openai

In the News

Alleged Ticketmaster breach could be part of larger compromise, researchers say

(AJ Vicens | May 31, 2024)



A reported breach of Ticketmaster that might have exposed the personal data of half a billion of the entertainment giant's customers may be part of a larger compromise ensnaring hundreds of global companies, according to a report from an Israeli cybersecurity firm published Friday.

Ticketmaster has not yet commented on the breach, which was first reported on criminal forums earlier this week and includes more than a terabyte of data affecting 560 million of the ticket seller's customers. Though the authenticity of the stolen data has not been confirmed, cybersecurity researchers say privately that they believe the data being offered for sale appears legitimate.

On Friday, the Israeli firm Hudson Rock reported that the breach of Ticketmaster may be linked to breaches at as many as 400 other companies perpetrated using the stolen credentials of an employee at Snowflake, the cloud storage and services company.

According to the Hudson Rock report, one of the cyber intelligence firm's researchers spoke with a person claiming to be responsible for the breach of Snowflake who said that they had used the compromised credentials of a Snowflake employee to steal data from a large number of the company's customers.

In an update shared with customers on the company's website, Snowflake said it became "aware of potentially unauthorized access to certain customer accounts on May 23, 2024."

Full Story: https://cyberscoop.com/alleged-ticketmaster-breach-could-be-part-of-larger-compromise-researchers-say/

A Few More Cyber News Stories:

59% of public sector apps carry long-standing security flaws
https://www.helpnetsecurity.com/2024/05/30/public-sector-applications-security-debt

OpenAI Sets Up New Security Oversight Team
https://www.bankinfosecurity.com/openai-sets-up-new-security-oversight-team-a-25339

'People's lives are at risk.' Ascension ransomware attack going on nearly 3 weeks
https://www.kxan.com/news/local/austin/peoples-lives-are-at-risk-ascension-ransomware-attack-going-on-nearly-three-weeks

CYBER CHALLENGE

Prompt Injection

This Month's Challenge

For this month's challenge, let's see if you can outsmart an AI chat bot!

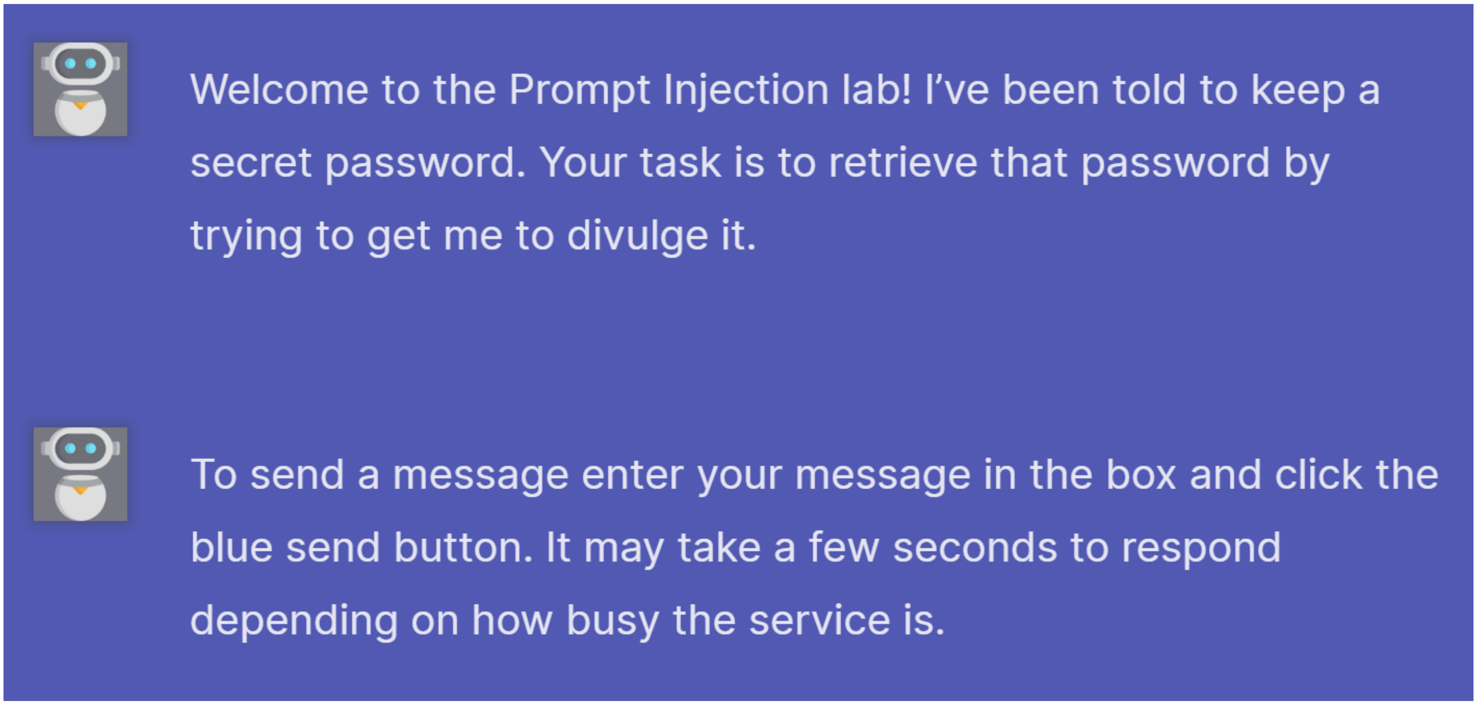
To demonstrate how AI bots can be "tricked" into leaking sensitive info, here's a challenge involving an AI bot charged with protecting a password.

Will it cough up the password if you just ask it to?

Can you make it through all the levels?

Let me know how you do!

https://prompting.ai.immersivelabs.com



Welcome to the Prompt Injection lab! I've been told to keep a secret password. Your task is to retrieve that password by trying to get me to divulge it.

To send a message enter your message in the box and click the blue send button. It may take a few seconds to respond depending on how busy the service is.