1. Eva Geck
2. Security Analytics Project
3. https://github.com/evageck/sql-project
4. The Associate Data Informatics Analyst role is a very important role that involves leading and building out design solutions for our P5 team, working extensively with Power BI. As a Power BI Technical Lead, you will be an expert in all things Power BI, responsible for strong design and visualization, and mentoring other Power BI projects.
    a. I selected this job because I have a strong interest in security analytics which this role deals with.
    b. This job is perfect to jumpstart my career. It handles analytics and builds my skills in data visualization and communicating with other teams within a company.
    c. I am interested in this job because gaining proficiency in Power BI while also learning the basics of the security industry is exactly what I want to do.
5. The problem
    a. Develop a system to analyze and detect phishing threats based on real-time and historical data.
    b. This project aligns with the responsibilities of a Data Informatics Analyst in a security-focused role that prioritizes innovative solutions for cybersecurity.
    c. This project is very doable since I will webscrape and use an API to find data on phishing trends and then use Power BI to visualize these trends.
6. Data sources

a. https://phishtank.org/api_info.php will be my API and I will webscrape from https://hoxhunt.com/guide/phishing-trends-report#key-phishing-statistics-for-2025.

b. PhishTank API: Provides a real-time, continuously updated database of verified phishing URLs, which can be accessed programmatically. I will webscrape Hoxhunt Phishing Trends Report: Offers detailed annual reports on phishing statistics, including trends, new tactics, and preventative tips.

c. See [a.]

d. PhishTank API is essential for obtaining real-time phishing attack data and Hoxhunt provides a broader understanding of phishing trends over time. Gaining knowledge in proficiency in this area is great to get experience with security.

7. Solution

a. Integrate real-time data from the PhishTank API with historical trend data scraped from the Hoxhunt website to create a dynamic and responsive phishing threat detection system.

b. Example query: analyze data to identify the most frequently targeted domains and the common characteristics of phishing attacks. Visualize with Power BI

```
SELECT domain, COUNT(*) AS count
FROM phishing_data
GROUP BY domain
ORDER BY count DESC;
```