Heimdal®

Methodology

We **collected the data manually** with the help of our data entry specialists, only from public posts on LinkedIn, Facebook, and Reddit and not through automated data-scraping tactics.

A total of **2,670 posts and comments** were reviewed to gather insights on job scams.

Next, we moved on to **data preprocessing**. This involved standardizing the text by converting everything to lowercase and removing special characters. We also cleaned the data to ensure all entries were usable and addressed any missing information.

With the data prepared, we **analyzed** it using **specialized techniques**:

- **Natural Language Processing (NLP**) - we defined, extracted and counted mentions of specific keywords.
- **Frequency Analysis** – we identified trends and patterns in the data.
- **Visualization** – we created visual representations of keyword mentions and other relevant data points.

Our analysis focused on **four main dimensions:**

- **Job Specifics** - we identified which industries and job levels were most targeted.

We looked for keywords such as "tech," "software," "developer" for the tech industry; "finance," "banking," "investment" for the finance industry; "healthcare," "nurse," "doctor" for the healthcare industry.

Terms like "entry-level," "manager," "senior," "mid-level" to determine which job levels were most targeted.

- **Scam Characteristics** – we examined common scam tactics.

We looked for keywords like "suspicious email," "non-professional contact," "unverified number."

Phrases such as "unrealistic salary," "high pay," "too good to be true."

Terms like "vague job description," "misleading offer," "fake job posting."

- **Impact on Victims** - assessed financial and emotional impacts on victims.

We looked for keywords such as "financial loss," "money stolen," "upfront payment."

Phrases like "identity stolen," "SSN requested," "personal information theft."

Terms like "distress," "anxiety," "anger," "helplessness."

- **Red Flags and Preventive Measures** – we identified common warning signs and recommended preventive measures.

We included keywords such as "upfront payment," "phishing," "confidential information request," "no interview."

Phrases like "check reviews," "verify company information," "consult with friends," "verify email domains."

(!) The analysis was conducted with the assistance of OpenAI's natural language processing capabilities. However, it is important to note that the analysis may have some limitations due to the automated processes involved, and the findings should be interpreted with these considerations in mind.