Design Thinking Project Workbook

Don't find customers for your product but find products for your customers

1. Team

Team Name: SPAM

Team Members:

Sathvik Choudary. T , Team Lead, 2320030235
Manaswi. CH , Team Member,2320030245
Sai Karthikeya. M , Team Member,2320030060

2. Problem/Opportunity Domain

Domain of Interest:

The domain of interest for this project is email communication management, specifically focusing on classifying emails as either spam or non-spam using machine learning and Natural Language Processing techniques.

Description of the Domain:

Email remains a primary communication tool for both personal and professional use. However, spam emails continue to flood inboxes, causing clutter and increasing security risks. These spam emails often contain unwanted content, phishing attempts, or malware. Sorting and managing this influx manually is time-consuming and inefficient. By automating the process of classifying emails as spam or non-spam, businesses and individuals can improve their productivity, security, and communication flow. Leveraging machine learning algorithms allows us to accurately detect and filter out spam emails without requiring extensive manual intervention.

Why did you choose this domain?

This domain was chosen because of the widespread impact that spam emails have on daily communication. Spam not only affects individual productivity but also poses significant security risks to organizations. Implementing an automated spam detection model is a practical and necessary solution that aligns with the team’s interest in utilizing machine learning and NLP to solve real-world problems.

3. Problem/Opportunity Statement

Problem Statement:
Users and organizations face a constant influx of spam emails, leading to cluttered inboxes, decreased productivity, and increased risks of phishing attacks. Developing a reliable model to classify emails as spam or non-spam can significantly improve email management, reduce security threats, and streamline communication.

Problem Description:
Spam emails are unsolicited and often contain harmful or irrelevant content. These emails flood users' inboxes, making it harder to find important messages. Manually filtering them is inefficient, especially with the large volumes many users receive daily. The problem is more critical for businesses, where failing to detect spam can lead to security breaches or financial loss.

Context (When does the problem occur):
The problem occurs continuously as spam emails are sent in large volumes daily, regardless of the user's activity. The issue intensifies during events like promotions, cyber-attacks, or phishing campaigns, where spam increases significantly.

Alternatives (What does the customer do to fix the problem):

- **Manual Filtering:** Users manually mark emails as spam, but this is inefficient and time-consuming.
- **Predefined Filters:** Email services offer basic filtering systems, but they often misclassify legitimate emails or fail to catch evolving spam techniques.
- **Third-party Tools:** Some users rely on external tools for spam filtering, but these tools may be expensive or not fully reliable.

Customers (Who has the problem most often):
The problem is commonly faced by anyone who uses email, especially organizations, e-commerce platforms, and service providers. High-volume email users, such as businesses, are particularly vulnerable to spam attacks and email clutter.

Emotional Impact (How does the customer feel):
Customers feel frustrated when spam floods their inboxes, especially if important emails are lost or buried. There is also anxiety over potential security threats from phishing emails disguised as legitimate communication.

Quantifiable Impact (What is the measurable impact):

- **Inbox Clutter:** Users spend more time sorting emails and risk missing important ones.
- **Security Risks:** Increased chances of falling victim to phishing attacks.
- **Reduced Efficiency:** Businesses face delays in communication due to time spent managing spam.

Alternative Shortcomings (What are the disadvantages of the alternatives):

- **Manual Filtering:** Time-consuming and inconsistent.
- **Predefined Filters:** Often inaccurate, leading to false positives or negatives.
- **Third-party Tools:** Can be expensive or not user-friendly, requiring additional setup.

Any Video or Images to showcase the problem:

No specific videos or images are available at this time. However, visual data such as workflow charts, email volume trends, and customer satisfaction survey results could be used to illustrate the problem and its impact more effectively during presentations or in reports.

4. Addressing SDGs

Relevant Sustainable Development Goals (SDGs):

The following SDGs are addressed by creating a model to classify emails as spam or non-spam:

- **SDG 9:** Industry, Innovation, and Infrastructure
- **SDG 12:** Responsible Consumption and Production

How does your problem/opportunity address these SDGs?

1. **SDG 9**: Industry, Innovation, and Infrastructure
   Developing an email classification model promotes using advanced technology to improve communication infrastructure. This project utilizes machine learning and NLP to modernize the digital infrastructure for more secure and efficient email management.

2. **SDG 12:** Responsible Consumption and Production
   By automating the email filtering process, we reduce time and energy spent on manually handling spam, optimizing resource use. This leads to more sustainable management of digital communication channels, promoting efficient information consumption

5. Stakeholders

1. Who are the key stakeholders involved in or affected by this project?

- **Email Users:** Individuals and businesses who benefit from better spam detection and email management.
- **Email Service Providers:** Companies that could integrate the spam detection model to improve their services.
- **Security Experts:** Responsible for ensuring the model effectively detects phishing emails or other threats.

Examples: organizations, educational institutions, etc…

2. What roles do the stakeholders play in the success of the innovation?

- **Email Users**: End users who provide feedback on the effectiveness of the spam filter.
- **Email Service Providers**: Implement and maintain the model, ensuring it scales and performs well.
- **Security Experts:** Ensure the system catches phishing and harmful emails accurately.

3. What are the main interests and concerns of each stakeholder?

- **Email Users:** Interested in a simple and effective solution. Concerned about accuracy and avoiding false positives.
- **Email Service Providers:** Interested in providing high-quality service to users while keeping operational costs low.
- **Security Experts:** Focused on ensuring the model is robust and capable of handling evolving spam techniques.

4. How much influence does each stakeholder have on the outcome of the project?

- **Email Users:** Medium influence through feedback and user experience.
- **Email Service Providers:** High influence, as they implement and support the system.
- **Security Experts:** High influence due to the importance of maintaining security.

5. What is the level of engagement or support expected from each stakeholder?

- **School Management**: High engagement, especially during the requirements-gathering phase, as they provide input on the kinds of inquiries the chatbot should handle.
- **College Management**: Moderate to high engagement, as they will be actively involved in testing and providing feedback.
- **Software Company**: Full engagement, as they will be responsible for the development, deployment, and maintenance of the chatbot.
- **Chemical Company**: Moderate engagement, providing essential information on technical queries and customer support automation needs.

6. Are there any conflicts of interest between stakeholders? If so, how can they be addressed?

Potential conflicts might arise between balancing user convenience and security requirements. Open communication and regular feedback loops will help address these conflicts by prioritizing both user experience and security.

7. How will you communicate and collaborate with stakeholders throughout the project?

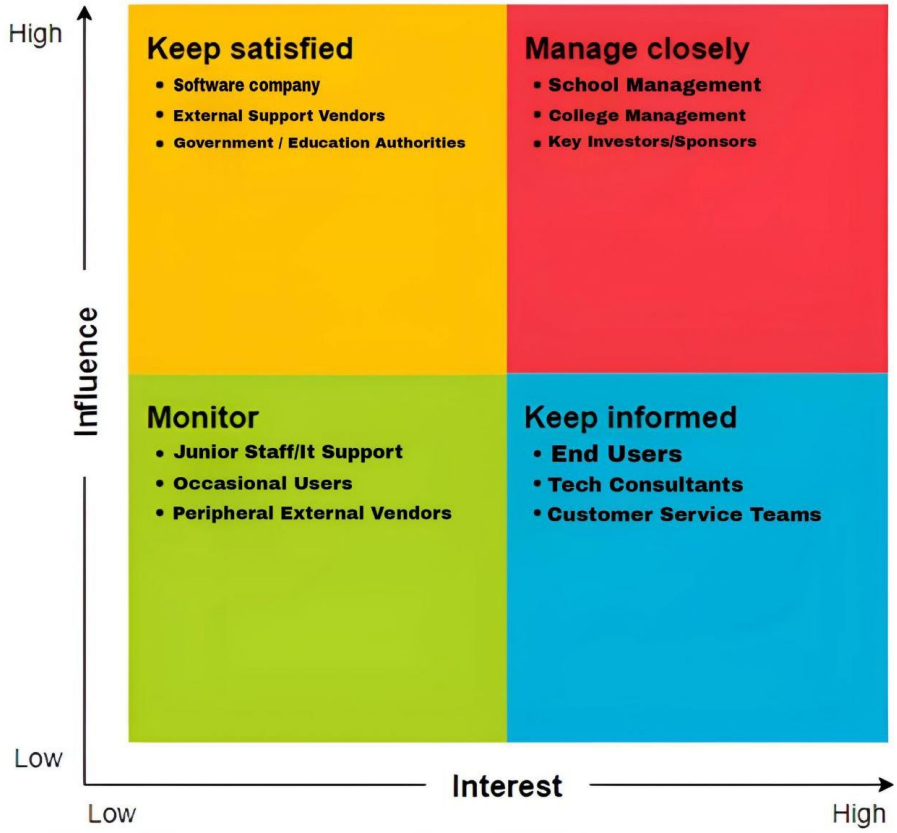
- **User Feedback:** Surveys or user testing sessions to gather feedback.
- **Regular Updates:** Email service providers will receive progress reports and updates.
- **Security Audits:** Regular reviews and tests with security experts to ensure robustness.

8. What potential risks do stakeholders bring to the project, and how can these be mitigated?

- **Email Users:** Risk of dissatisfaction if the system misclassifies emails. Mitigation: Regular tuning of the model based on feedback.
- **Email Service Providers:** Risk of system failure or inefficiency. Mitigation: Thorough testing before deployment.
- **Security Experts:** Risk of security vulnerabilities. Mitigation: Continuous updates to detect new types of spam or threats.

6. Power Interest Matrix of Stakeholders

Power Interest Matrix:



High Power, High Interest:

- **Email Service Providers:** They have significant influence on the success of the project as they are responsible for implementing and maintaining the email classification system. Their involvement is critical since they manage the infrastructure where the model will operate.

High Power, Low Interest:

- **IT Departments:** They have the power to implement and manage the system but may not have a direct, day-to-day interest in the specific classification model itself, as their focus might be on broader infrastructure tasks.

Low Power, High Interest:

- **Email Users (Businesses and Individuals**): While they may not have a lot of power to influence the design or technical aspects, they are highly interested in ensuring that the spam filter works efficiently to prevent spam and phishing emails without misclassifying important messages.

Low Power, Low Interest:

- **Non-Business Email Users:** These users interact with email on a more casual level and are less likely to be affected by spam-related issues or have any direct influence on the design of the model.