International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 14 Issue 1, January-2025

E - Mail Spam Detection Using Design Thinking

Lakshana Sree K L

SNS College of Technology, Coimbatore

ABSTRACT

Email has become a vital communication tool in both personal and professional contexts. Sensitive details such as passwords, credit card information, and banking credentials are often shared via email, making them prime targets for cybercriminals. Fraudsters commonly use deceptive emails posing as legitimate organizations to trick users into divulging personal information. This tactic, known as phishing, involves sending emails that appear authentic but are designed to steal sensitive data. This paper investigates the classification of phishing emails and explores machine learning techniques to enhance their detection. Experimental results lay the groundwork for addressing this critical issue.

Keywords: Spam detection, phishing emails, email fraud, machine learning.

INTRODUCTION

Phishing has emerged as a significant and rapidly evolving cybersecurity threat in today's digital age. It combines social engineering and technical manipulation to deceive individuals into sharing sensitive information such as usernames and passwords (Manning & Aron, 2015) [1]. According to Lungu and Tabusca (2010) [2], the rise in cyberattacks and data breaches has significantly impacted the global economy. Phishing, including malicious websites, phishing emails, and malware, has been classified based on its method of execution (Jain & Richariya, 2011) [3].

Phishing emails are particularly dangerous as they often masquerade as messages from reputable organizations, such as banks, prompting users to click on malicious links. Clicking such links redirects victims to fraudulent websites designed to steal credentials or financial details (Al-Momani & Gupta, 2013) [4]. The phishing lifecycle typically begins with a deceptive email, aiming to lure recipients into clicking the link, similar to a fisherman casting a net to catch unsuspecting prey.

Phishers employ two primary techniques: **deceptive phishing** and **malware-based phishing** (Fig. 2). The deceptive method relies on social engineering to send misleading emails with fake links, leading recipients to fraudulent sites requesting sensitive information. On the other hand, malware-based phishing uses harmful software to exploit vulnerabilities in the user's system, gaining unauthorized access to accounts or stealing information (Al-Momani, 2013) [5]. In 2012, phishing scams caused an estimated $1.5 billion in losses. This growing threat necessitates the development of more robust detection techniques to counteract the damage.

DESIGN THINKING

Design Thinking is a user-centric, iterative problem-solving approach that combines empathy, creativity, and rationality to address complex challenges. It emphasizes understanding the user's needs, redefining problems, and creating innovative solutions through a structured yet flexible process. This methodology has gained prominence across industries due to its focus on collaboration and its ability to foster practical, user-friendly outcomes.

The core of Design Thinking lies in its five stages: **Empathize, Define, Ideate, Prototype, and Test**. In the **Empathize** stage, researchers immerse themselves in the user's world to identify pain points and unmet needs. The **Define** phase involves synthesizing these insights into a clear and actionable problem statement. **Ideation** fosters creativity, encouraging brainstorming sessions to generate diverse ideas and potential solutions. The **Prototype** stage focuses on building tangible models or systems to test these ideas in a practical setting. Finally, in the **Test** phase, feedback is gathered from users to refine and enhance the solution, ensuring its effectiveness and relevance.

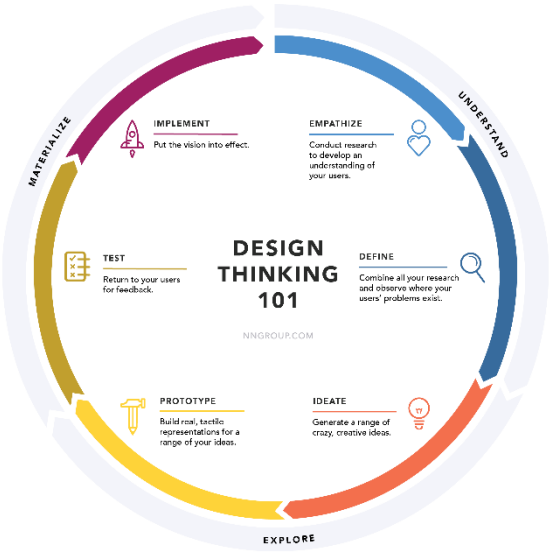

Fig 1: Stages of Design Thinking

Design Thinking is particularly effective in tackling issues where traditional methods fall short, as it encourages out-of-the-box thinking and iterative learning. It allows for innovation while maintaining a focus on user satisfaction. By aligning solutions with user requirements and continuously refining them, Design Thinking ensures that the final product is both impactful and efficient.

EMPATHIZE

The increasing prevalence of phishing and spam emails has caused significant distress for email users and organizations alike. Users often struggle to identify fraudulent emails, which leads to security breaches, financial losses, and unauthorized access to sensitive data. Traditional methods, such as blacklists and basic heuristics, fail to adapt to the constantly evolving tactics employed by cybercriminals. These limitations create a pressing need for more reliable and user-friendly solutions. Similarly, organizations face mounting pressure to safeguard their digital infrastructure and prevent reputational damage caused by phishing attacks. A comprehensive understanding of these challenges reveals that users and organizations both require a system that balances robust security with an intuitive experience

DEFINE

The core problem lies in the inability of existing systems to effectively detect phishing emails, especially as attackers continue to develop more sophisticated techniques. Current solutions, while helpful to some extent, often lack the adaptability required to counter these dynamic threats. The objective of this research is to create a spam detection system that identifies phishing attempts with precision while minimizing errors, such as falsely marking legitimate emails as spam. By leveraging advanced machine learning methods, the proposed solution seeks to adapt dynamically to new phishing techniques, ensuring both security and user convenience.

Key Objectives:

- To develop a spam detection system that can adaptively identify phishing emails with high accuracy.
- To minimize user inconvenience by reducing false positives and negatives.
- To incorporate machine learning techniques that evolve with the changing tactics of attackers.

IDEATE

To address the challenges of spam detection, innovative approaches are necessary. Machine learning offers the potential to analyze email features, such as sender details, content structure, and embedded links, to accurately classify messages. Algorithms like Random Forest, Naive Bayes, and Support Vector Machines can be utilized to improve detection rates by identifying patterns in phishing emails. A multi-layered filtering system could further enhance performance, with separate layers dedicated to indexing, topic analysis, and content-type filtering. Additionally, incorporating a user feedback loop can

help refine the system over time by allowing users to report misclassified emails. These ideas aim to create a comprehensive and adaptive spam detection framework that meets real-world demands.

Key steps include:

- **Data Preprocessing:** Collect and clean datasets with diverse examples of phishing and legitimate emails.
- **Feature Extraction:** Identify key characteristics, such as suspicious keywords, malicious links, and abnormal sender details.
- **Algorithm Implementation:** Apply machine learning algorithms like Random Forest and Naive Bayes to analyze and classify emails.
- **User Interface Design:** Develop a simple email interface showing spam scores and providing options for users to review flagged emails.

PROTOTYPE

The prototype for the spam detection system integrates several key components to ensure functionality and effectiveness. Initially, the system preprocesses data by cleaning and organizing a dataset comprising examples of legitimate, spam, and phishing emails. Key features, such as keywords, URL structures, and metadata, are extracted and analyzed using machine learning algorithms like Random Forest and Naive Bayes. The system is designed to classify emails into categories and display results through an intuitive interface, which provides users with clear spam scores and options for manual review. This prototype is a starting point for testing and refinement, ensuring the system meets its goal of accurate and reliable spam detection.

TEST

The testing phase evaluates the prototype using real-world data to ensure its accuracy and practicality. Metrics such as detection rates and false positives are analyzed to measure the system's performance in identifying phishing emails. Feedback from users is collected to refine the interface and improve usability, ensuring the system remains easy to navigate while effectively protecting against threats. Testing also involves stress-testing the system with a variety of phishing techniques to assess its adaptability and robustness. By iterating on the feedback and performance metrics, the spam detection system evolves into a highly effective solution that addresses the needs of users and organizations alike.

REFERENCES

[1] Verizon, *Data Breach Report 2016*.
[2] Akinyelu, A.A., & Adewumi, A.O. *Classification of Phishing Emails Using Random Forest Machine Learning Technique*, 2014.
[3] Jameel, N.G.M., & George, L.E. *Detection of Phishing Emails Using Feed-Forward Neural Networks*, *International Journal of Computer Applications*, 2013.
[4] Fette, I., Sadeh, N., & Tomasi, A. *Learning to Detect Phishing Emails*, Proceedings of the International World Wide Web Conference (WWW), 2006.
[5] Gori Mohamed J., M. Mohammed Mohideen, and Mrs. Shahira Banu, *Email Phishing – An Open Threat to Everyone*, *International Journal of Scientific Research Publications*, 2014.
[6] Emilin Shyni C., Sarju S., and Swaminathan S., *A Multi-Classifier Based Prediction Model for Phishing Emails Detection Using Topic Modelling, Named Entity Recognition, and Image Processing*, *SciRes*, 2016.
[7] Noor Ghazi M. Jamee and Loay E. George, *Detection of Phishing Emails Using Features Decisive Values*, 2014, pp. 257-259.
[8] Rakesh M. Verma and Nirmala Rai, *Phish-IDetector: Message-Id Based Automatic Phishing Detection*, *International Joint Conference on e-Business and Telecommunications*, 2015.
[9] Basnet R., Mukkamala S., and Sung A.H., *Detection of Phishing Attacks: A Machine Learning Approach*. In: Prasad B. (Ed.), *Soft Computing Applications in Industry*, *Studies in Fuzziness and Soft Computing*, Vol. 226, Springer, Berlin, Heidelberg, 2008.