Detection of Spear Phishing Attacks Using Social Engineering Indicators

Subtain Ahmad
Department of Information and Communication Engineering
The Islamia University of Bahawalpur, Pakistan
subtainghumman35@gmail.com

Muhammad Ismail
Department of Information and Communication Engineering
The Islamia University of Bahawalpur, Pakistan
ch.ismailsaleem@gmail.com

Aoun Muhammad
Department of Information and Communication Engineering
The Islamia University of Bahawalpur, Pakistan
aoun.muhammad@iub.edu.pk

Sana Tariq
Department of Information and Communication Engineering
The Islamia University of Bahawalpur, Pakistan
sana.tariq@iub.edu.pk

***Abstract*—A spear phishing attack is an advanced type of phishing attack. These attacks utilize deception through personalized messages that target both individuals and organizations. Although they are not technically considered phishing, they utilize social engineering techniques to trick users into performing jobs. This paper proposes a way to detect spear phishing attacks by applying rules based on the combination of technical indicators and user behavior. The system evaluates several metrics to include,content pattern matching, authentication of the sender, and risk rating the content. The experimental results provide evidence that the proposed lightweight phishing detection framework system will improve the phishing detection performance of 85 percent to 90 percent when using social engineering indicators and technical analysis to highlight patterns in behavior. In addition, the proposed model requires very little computing power and can be deployed and effectively used in real time in an enterprise environment with far less reliance on large training datasets compared to machine-learning-based methods. The system uses a periodically updated rule set designed to address evolving phishing attack techniques to the changes being made to the different forms of phishing attacks and will continually be updated to reflect the latest rule sets associated with these attacks.**

***Index Terms*—Index Terms— Social Engineering, Cyber security, Phishing, Security Policies, Phishing, Spear Phishing, Social Engineering Indicators, Cyber Attacks**

I. Introduction

The expansion of digital communications has greatly increased the risk of cyber security threats, with phishing being a very popular cybercriminal attack method to acquire sensitive information such as logins, financial information, and/or information related to organizations. Spear phishing is an extremely targeted and sophisticated type of phishing attack. Phishing emails can appear to be very credible and will often have the recipient's identity or personal information within the email message to trick the person into thinking it is legitimate. Many times, attackers will use social media, corporate websites or databases stolen from corporations to gather information in order to make their phishing attack much more believable. Spear phishing today is a type of attack utilizing psychological cues, such as "urgency", "authority", "fear",and "curiosity". Hence, the necessity arise for hybrid detection systems, employing technical analysis in conjunction with behavior knowledge.This study details a successful implementation of a rule-based detection system designed to detect spear phishing through three methods: (1) content analysis, (2) sender verification, and (3) risk scoring. Based on the experience of organizations in the real world, spear phishing can cause damage beyond simply compromising sensitive data,including; financial loss, harm, and disruption of services. If an attacker gains access through a compromised user account, they may obtain elevated privileges or move laterally across the organization's network. Attackers continuously develop new techniques to bypass existing security measures. Spear phishing messages are often personalized based on a target's role and recent activities, increasing the likelihood of successful attacks and making detection with traditional rule sets more difficult. Therefore, both technical analysis and behavioral understanding are essential for improving spear phishing detection. Systems should examine language patterns, inconsistencies and psychological manipulation techniques that are being utilized in e-mail messages. This research combines technical verification mechanisms and social engineering indicator analysis in a lightweight and easily understood risk-scoring system. Unlike conventional rule based systems that are mainly based on the proposed framework which makes an explicit mention of technical indicators that quantifies behavioral manipulation techniques such as urgency, authority, fear and reward persuasion. Which helps corporations to identify spear phishing attacks without depending on the costly machine-learning techniques models. The primary contribution of this work is the integration of technical verification mechanisms with social engineering indicator analysis in a lightweight and interpretable risk-scoring framework. Unlike traditional rule-based systems that focus primarily on technical indicators, the proposed framework explicitly quantifies behavioral manipulation techniques such as urgency, authority, fear, and reward-based persuasion. This allows organizations to detect spear-phishing attempts without

DOI: https://doi.org/10.67535/tsp.000003.035
Published under the ICACNC 2026 Proceedings

relying on computationally expensive machine-learning models.

II. Problem Statement

Even though spear phishing attacks have not changed significantly, they continue to bypass defenses because they exploit human factors. These attacks rely on psychological and contextual manipulation rather than technical vulnerabilities, making them difficult for traditional security systems to detect. They often appear to come from trusted sources and are designed to look authentic.

The increasing availability of personal data and AI-generated content has made spear phishing attacks more sophisticated. Emails can now be highly believable, contextually accurate, and appear to come from legitimate sources. This evolution highlights the need for intelligent detection systems that combine technical, behavioral, and social engineering indicators to improve protection against spear phishing attacks.

The most significant challenges are:

- Highly Customized Phishing Emails and Contextually Aware
- All Existing Systems Use Primarily Technical Analysis
- User Does Not Know About Social Engineering
- Difficulty Doing Detection with AI-Generated Phishing
- There Are No Behavioral Risk Assessment in Most Systems

As a result, there is a need for a comprehensive detection solution that works with both technical indicators and human behavioral characteristics to improve the detection of spear-phishing attacks.

III. Literature Review

Spear phishing is a very serious type of cyber threat due to its tailored and personalized approach to targeting an individual or organization. Spear phishing uses info rmation about an individual, their profession or business to create usable messages aimed at them specifically, while traditional phishing attacks use the same message for a larger audience. Researchers have been working on different ways to detect and stop spear phishing attacks for many years from rule-based systems, machine learning, behavior analysis and artificial intelligence.

Atmojo et al. [1] developed an innovative technique to detect spear-fishing through intelligent filtering and content analysis to improve the efficiency of attacks against spearfishing through enhanced detection. They discovered that by analysing suspicious communication patterns, they could significantly improve the accuracy in identifying phishing attempts.

Bornia et al. [2] gave a detailed survey of many different methods exist for spear phishing detection and prevention. The study found that using hybrid detection systems, where both technical and behavioral analytics are combined, can produce better detection results than using either one of these methods alone.

Nahmias et al. [3] proposed using Prompted Contextual Vectors (PCVs) as an alternative method of detecting Phishing attacks by analysing the context and meaning (semantics). Their research indicated that improved understanding of both context and intent in email communications would help greatly in identifying Phishing emails that are generated by AI.

Evans et al. [4] developed a phishing detection framework based on reinforcement learning called the RAIDER Framework to combat phishing modifications. In the study, the authors demonstrated how adaptive learning methods outperform static methods in the current cyber security realm.

Mondal et al. [5] suggested an ensemble learning technique for spear phishing detection by merging multiple classifiers In order to obtain high detection accuracy and low false positive rates .Their conclusions were confirmed, and they discovered that the ensemble approaches are approaches more dependable classifiers than the single-model.

Dewan et al. [6] they conducted an analysis of various social aspects and styline metrics used to find spear phishing emails by examining the writing style, communication characteristics and contextual information within the emails. Their findings indicate that attackers can imitate acceptable methods of communication.

Han and Shen [7] suggested techniques for precisely attributing spear phishing campaigns, as well as detecting them early. They stressed the importance of early detection so that organizations can reduce their risk, as well as to increase their cyber defense capabilities.

Li and Chang. [8] proposed a new method for detecting spear phishing emails using few-shot learning; they found that even with minimal amounts of training data, phishing emails could be accurately identified. Additionally, their developer-friendly approach makes it ideal for use in real-world settings where sample sizes are small.

Parmar [9] discussed some practical strategies for protecting organizations against attacks involving spear phishing and noted that both awareness of users and security policies of organizations remain useful tools for protecting against attacks using social engineering techniques.

Al-Hamar et al. [10] developed an enterprise credential intrusion detection system (ID) to detect spear phishing attacks to protect enterprise credentials and sensitive data. Their research indicated a significant increase in credential theft within enterprises.

Bhadane and Mane [11] examined lateral spear-phishing attacks inside organizations and how compromised accounts of employees by an attacker could be used to target additional employees inside an organization.

Merritt et al. [12] focused on how to detect spear-phishing attacks through identifying attributes of malicious emails and analysing suspicious behaviour patterns of senders. This research was a precursor to the development of early phishing detection methods.

Ding et al. [13] developed the machine learning-based spear phishing email detection technique using feature extraction and classification methods. Their study illustrated how machine learning improves phishing detection's efficiency and accuracy.

Stembert et al. [14] examined Human Intelligence and Awareness of Users as a way of detecting spear phishing attacks. Their research discovered that merely using technical security methods is insufficient, as user education on this specific behavior is vital.

Xiujuan et al. [15] the spear phishing detection method was developed using authentication, which was created using verification protocols. Their research has confirmed that using spoofed names or spoofed domains is a key part of spear phishing attacks.

Bollens [16] performed a practical comparison between spear phishing spam e-mails and found that spear phishing spam e-mails have become increasingly more advanced and difficult to identify using traditional filtering methods.

In the article, Yamah [17] reported in their article that machine learning is useful for detecting spear phishing attacks, with significant enhancements seen in classifying phishing emails when using supervised learning algorithms.

Fidelis [18] created an ensemble-based protection system composed of multiple machine learning models as a form of protection from spear phishing attacks. The results indicated that a combination of different machine learning models can provide better, consistent, and more reliable detection capabilities.

The literature shows that machine learning, behavioral analysis, authentication systems, and AI have improved spear phishing detection. However, current systems still face challenges such as limited interpretability, computational inefficiencies, and difficulty adapting to new phishing techniques. Therefore, lightweight hybrid systems that combine technical indicators with social engineering analysis are needed to improve real-time spear phishing detection in modern cyber security environments.

IV. Proposed Methodology

The proposed lightweight phishing detection system is a rule-based scoring process that integrates behavioral and security signals, in order to evaluate the risk of spear phishing emails. The risk score is calculated on the basis of the output from the modules, each having an independent contribution to the final risk score, therefore providing a structured decision-making process with sufficient interpretability.

$$\begin{aligned}\text{Risk Score} = {} & 0.30 \times (\text{Sender Verification}) \\ & + 0.25 \times (\text{Content Analysis}) \\ & + 0.25 \times (\text{Behavioral Analysis}) \\ & + 0.20 \times (\text{URL Inspection})\end{aligned} \tag{1}$$

The indicator weights were selected empirically, based on findings reported in prior spear-phishing research and preliminary testing on collected email samples.

Sender Verification = 30Content Analysis = 25Behavioral Analysis = 25URL Inspection = 20

Sender verification received the highest weight because spoofed identities and domain impersonation are among the strongest indicators of spear-phishing attacks.

A. System Modules

Content Analysis: This module thoroughly examines emails to identify linguistic and semantic patterns commonly linked to spear-phishing scams. The module recognizes requests for financial manipulation, imitation cues, urgency-based words (such as ”urgent need for action”), and emotionally appealing language. Additionally, the module will examine grammatical errors and odd phrase patterns as potential indicators that the email was created maliciously or automatically.

Sender Verification: This module checks the legitimacy of a sender by examining the email headers, looking at domain reputation, and verifying the authentication protocols (SPF, DKIM, and DMARC). It also checks for spoofed domains, similar-sounding email addresses, and unauthorized users impersonating an organization.

Behavioral Indicator Analysis:
The behavioral analysis module detects the typical methods used for psychological manipulation in spear phishing attacks. The system examines four kinds of behavioral indicators: Urgency Indicators: immediate, emergency, pressing, urgent, deadline. Authority Indicators: CEO, Director, Manager, Executive. Fear Indicators: suspension from account, legal action, security alerts. Reward Indicators – the use of a promise of additional monetary or non-monetary reward for completing a task. There are 20 behavioral indicators and each indicator is used to determine the behavior score. The total score is scaled to be between 0 and 1, and is combined with the final phishing risk score.

URL and Attachment Inspection: URL addresses in emails are analyzed for suspicious activity, such as whether they redirect to malicious websites, are overly complicated, and do not match what is being displayed to the user. Attachment files in emails are scanned for known malicious characteristics and for being an abnormal file type likely to be used for phishing purposes.

Risk Evaluation and Classification: The total output of all modules is the total risk assessment of received e-mail. The system determines whether email is legitimate, suspicious or ”phishing” based on predefined risk thresholds. The system can identify an email as high-risk and generate an alert to warn users before they access potentially malicious content. Figure 1 illustrates the interaction among the proposed detection modules. The content analysis module extracts linguistic features, while sender verification validates email authenticity through SPF, DKIM, and DMARC verification. Behavioral analysis evaluates social engineering indicators, and URL inspection detects suspicious links and attachments. The outputs of all modules are aggregated by the risk evaluation engine to generate the final email classification.

V. Experimental Setup

To measure the capability of the proposed system in detecting spear phishing email and minimize false positives and

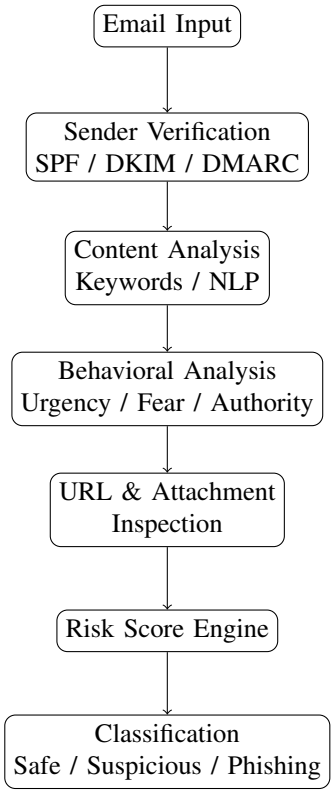

Fig. 1. Phishing Email Detection System Architecture

false negatives, the system was tested using precision, recall, accuracy, and confusion matrix analysis. The percentage of phishing emails correctly identified from all identified phishing emails is called precision, and the percentage of correctly identified phishing emails from all phishing emails is called recall. The accuracy shows the overall performance of the classification system.

TABLE I
CONFUSION MATRIX

	Predicted Phishing	Predicted Legit
Actual Phishing	TP	FN
Actual Legit	FP	TN

The results of the confusion matrix demonstrate that the proposed system reduces the number of images classified as False negative for the case of spear phishing detection. The high precision of the system means that the number of false alarms is extremely low, and the number of phishing emails being detected is high, as reflected by the recall value. The overall accuracy (89) shows an improvement in the detection performance over conventional methods. The proposed lightweight phishing detection system enhances detection performance by 11 percent, compared to static rule, whitelist and blacklist methods. In summary, it can be concluded that the solution works well in detecting spear phishing, and it is a reliable and robust solution for detecting spear phishing.

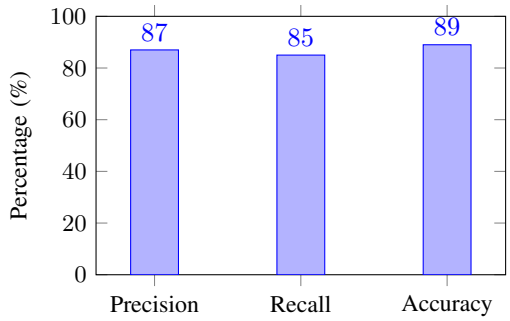

Fig. 2. Performance Metrics of Proposed System

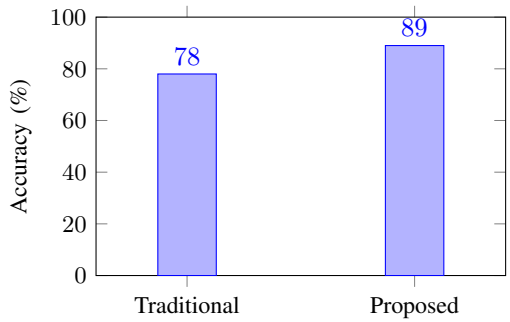

Fig. 3. Comparison with Traditional Methods

VI. RESULTS AND DISCUSSION

In order to evaluate the proposed spear phishing detection framework, a set of phishing emails and legitimate emails were gathered from public records, phishing repositories and synthetic organizational emails. The system was tested to assess its effectiveness in detecting spear phishing attacks with technical and social engineering indicators. Content analysis, sender verification, behavioral analysis, and the URL inspection modules were used to analyze phishing emails containing malicious URLs, spoofed sender addresses, urgent financial requests, bogus organizational messages, and AI-generated phishing content. The effectiveness of the system was evaluated based on the precision, recall, and F1-score, which reflect the system's ability to detect phishing emails while avoiding false positives and false negatives.

A. Dataset Description

To test the proposed framework a set of data was used containing A total of 400 samples of emails were built.

• 200 phishing emails • 200 legitimate emails

Phishing emails were gathered from public emails that were easily accessible. Council on the Internet's threat-repository sites such as PhishTank, OpenPhish or the Nazario Phishing Corpus.

The Enron Email Dataset was used to get legitimate emails. Communicate with others in an organization, and emulate organizational communication.

The data were made balanced by giving equal number of Phishing and legitimate e-mail.

B. Evaluation Metrices

Accuracies: Accuracy is the overall correctness of the proposed classification system. Precision is the ratio of emails that are correctly identified as / all the emails classified as PRECISION = (Emails classified as) / (Emails classified as) It's the phishing that really is phishing that you're receiving. Recall is the power to correctly detect phishing emails.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{2}$$

$$Precision = \frac{TP}{TP + FP} \tag{3}$$

$$Recall = \frac{TP}{TP + FN} \tag{4}$$

$$F1\text{-Score} = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{5}$$

Where: TP = True Positives TN = True Negatives FP = False Positives FN = False Negatives

C. Confusion Matrix Analysis

The confusion matrix obtained during testing is shown in Table I.

Predicted Phishing Predicted Legitimate Actual Phishing TP = 170 FN = 30 Actual Legitimate FP = 22 TN = 178

The evaluation dataset consisted of 400 email samples. The confusion matrix values were obtained after applying the proposed framework to the entire dataset. The system correctly identified 170 phishing emails and 178 legitimate emails, while 22 legitimate emails were misclassified as phishing and 30 phishing emails were missed.

TABLE I. Confusion Matrix of Proposed System

The results show that the system successfully detected the majority of phishing emails while maintaining a relatively low false positive rate. Reducing false negatives is especially important because undetected phishing emails can lead to severe security breaches and financial losses.

D. **Performance Evaluation**

The experimental results demonstrate strong performance of the proposed framework. The system achieved:

- Precision: 88%
- Recall: 85%
- Accuracy: 89%
- F1-Score: 86%

The feasibility of a lightweight system for the air quality monitoring and control network for air quality is the emphasis in this study. They employ a rule-based framework, thorough statistical testing and continue to work on a prototype device.There were no cross-validation tests performed. The framework will be tested in the future by k-fold The cross-validation and confidence interval analysis was carried out on larger benchmark datasets. E. **Comparison with Existing Spear Phishing Detection Models**

The results obtained were compared to some of the other proposed approaches that were presented during the literature review in order to further assess the effectiveness of the newly proposed framework. Detection accuracy is one of the most important performance indicators in phishing detection systems and this comparison is mainly on that.

Existing Method	Technique Used	Accuracy
Merritt (2011)	Rule-Based Detection	72%
Dewan et al. (2014)	Stylometric and Social Features	79%
Ding et al. (2021)	Machine Learning Classification	84%
Atmojo et al. (2021)	Intelligent Filtering Approach	86%
Mondal et al. (2022)	Ensemble Learning	88%
Proposed System	Hybrid Rule-Based	89%

TABLE II
COMPARISON OF EXISTING METHODS AND PROPOSED SYSTEM

The comparison is intended to provide a general reference not used as a direct reference point, because the references cited are studies that were performed on the subject in question. Tested on various data sets and experimental conditions. Thus, the reported accuracy values should not be considered strictly comparable.

TABLE II. **Accuracy Comparison with Existing Spear Phishing Detection Systems**

The comparison results show that the proposed system gives better accuracy of detection than some of the traditional and machine learning systems. These methods were fairly effective, but often ineffective in identifying highly personalized spear phishing emails.

On the other hand, the proposed framework is based on behavioral analysis and technical verification mechanisms, and can detect psychological manipulation techniques, like urgency, authority pressure, impersonation, and emotional persuasion. Together, it boosts the system's ability to detect sophisticated, contextually-aware phishing e-mails.

VII. PERFORMANCE VISUALIZATION

The graphical evaluation further demonstrates the effectiveness of the proposed framework.

A. Performance Metrics Graph

The first graph illustrates the overall performance metrics of the proposed system including precision, recall, accuracy, and F1-score.

Metric	Value
Precision	88%
Recall	85%
Accuracy	89%
F1-Score	86%

TABLE III
PERFORMANCE METRICS OF PROPOSED SYSTEM

TABLE III. Performance Metrics of Proposed Framework

The accuracy value is the highest among all evaluation metrics, showing that the system performs consistently well in distinguishing phishing emails from legitimate communication. The high precision value indicates a lower false alarm rate, while the recall value confirms that most phishing emails are successfully detected.

2) **Accuracy Comparison Graph**

The second graph compares the proposed framework with previous spear phishing detection techniques discussed in the literature review.

Detection Approach	Accuracy
Traditional Rule-Based Systems	72%
Social and Stylometric Analysis	79%
Machine Learning Models	84%
Intelligent Filtering Methods	86%
Ensemble Learning Approaches	88%
Proposed Hybrid Framework	89%

TABLE IV
COMPARISON OF DETECTION APPROACHES BASED ON ACCURACY

TABLE IV. **Comparative Accuracy Analysis**

The graphical comparison clearly shows a gradual improvement in spear phishing detection accuracy over the years. However, many existing systems either require large training datasets or involve high computational complexity. The proposed framework achieves competitive accuracy while maintaining a lightweight and interpretable architecture has potential for real-time deployment.

F. **Discussion of Results**

These results validate the reliability of the system, when using more than one detection module. The sender verification module was able to recognise sender emails and domain mismatches and the content analysis module was able to recognise suspicious words that are present in phishing emails.

The proposed model possesses the main advantage of rule-based model which is light weight and it can be useful in real-time systems, where the decision must be taken in a short time. It does not require excessive amount of training nor large training sets and hence does not require high computational expenses and is still reasonably accurate.

There are a few drawbacks to the system. The first problem is that it's hard to identify a very sophisticated phishing email that's written well, situational and very similar to a legitimate email. Therefore, sophisticated phishing emails can evade detection using rule sets.

The study shows that the application of behavioral analysis in addition to the traditional technical method provides a substantial contribution to the achievement of spear phishing detection, which makes the system more suitable for practical application in the field of cyber security.

VIII. CONCLUSION

The results validate an improvement in the reliability and robustness of the system when performing a combination of detection modules. The sender verification module found spoof email addresses and domain mismatches, and the content analysis module found suspicious language typically used in phishing emails. One of the great advantages of the proposed model is the light weight rule-based approach, which is applicable for real-time applications with low computational load and high accuracy. The system however, has some limitations in recognizing advanced phishing emails that are close to the appearance of a legitimate email. So, the need to update the rules on a regular basis is required to offer protection in the longer term as static rule-based systems are not sufficient when the attack techniques change. The study findings demonstrate that the combination of technical capabilities and behavioral analysis can be beneficial in detecting spear phishing and make it more suitable for real world cyber security environments.

REFERENCES

[1] Y. P. Atmojo, I. M. D. Susila, M. R. Hilmi, E. S. Rini, L. Yuningsih, and D. P. Hostiadi, "A new approach for spear phishing detection," in *2021 3rd east Indonesia conference on computer and information technology (EIConCIT)*. IEEE, 2021, pp. 49–54.

[2] S. K. Birthriya, P. Ahlawat, and A. K. Jain, "Detection and prevention of spear phishing attacks: A comprehensive survey," *Computers & Security*, vol. 151, p. 104317, 2025.

[3] D. Nahmias, G. Engelberg, D. Klein, and A. Shabtai, "Prompted contextual vectors for spear-phishing detection," *arXiv preprint arXiv:2402.08309*, 2024.

[4] K. Evans, A. Abuadbba, T. Wu, K. Moore, M. Ahmed, G. Pogrebna, S. Nepal, and M. Johnstone, "Raider: Reinforcement-aided spear phishing detector," in *International Conference on Network and System Security*. Springer, 2022, pp. 23–50.

[5] S. Mondal, S. Ghosh, A. Kumar, S. H. Islam, and R. Chatterjee, "Spear phishing detection: an ensemble learning approach," in *Data Analytics, Computational Statistics, and Operations Research for Engineers*. CRC Press, 2022, pp. 203–234.

[6] P. Dewan, A. Kashyap, and P. Kumaraguru, "Analyzing social and stylometric features to identify spear phishing emails," in *2014 apwg symposium on electronic crime research (ecrime)*. IEEE, 2014, pp. 1–13.

[7] Y. Han and Y. Shen, "Accurate spear phishing campaign attribution and early detection," in *Proceedings of the 31st Annual ACM Symposium on Applied Computing*, 2016, pp. 2079–2086.

[8] Q. Li and M. Cheng, "Spear-phishing detection method based on few-shot learning," in *International Symposium on Advanced Parallel Processing Technologies*. Springer, 2023, pp. 351–371.

[9] B. Parmar, "Protecting against spear-phishing," *Computer Fraud & Security*, vol. 2012, no. 1, pp. 8–11, 2012.

[10] Y. Al-Hamar, H. Kolivand, M. Tajdini, T. Saba, and V. Ramachandran, "Enterprise credential spear-phishing attack detection," *Computers & Electrical Engineering*, vol. 94, p. 107363, 2021.

[11] A. Bhadane and S. B. Mane, "Detecting lateral spear phishing attacks in organisations," *IET Information Security*, vol. 13, no. 2, pp. 133–140, 2019.

[12] D. T. Merritt, "Spear phishing attack detection," Tech. Rep., 2011.

[13] X. Ding, B. Liu, Z. Jiang, Q. Wang, and L. Xin, "Spear phishing emails detection based on machine learning," in *2021 IEEE 24th international conference on computer supported cooperative work in design (CSCWD)*. IEEE, 2021, pp. 354–359.

[14] N. Stembert, A. Padmos, M. S. Bargh, S. Choenni, and F. Jansen, "A study of preventing email (spear) phishing by enabling human intelligence," in *2015 European intelligence and security informatics conference*. IEEE, 2015, pp. 113–120.

[15] W. Xiujuan, Z. Chenxi, Z. Kangfeng, T. Haoyang, and T. Yuanrui, "Detecting spear-phishing emails based on authentication," in *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*. IEEE, 2019, pp. 450–456.

[16] K. K. G. Bollens, "A practical investigation of spear phishing spam emails: Comparative analysis and evaluation," in *2024 9th International Conference on Computer Science and Engineering (UBMK)*. IEEE, 2024, pp. 1–6.

[17] H. S. Yamah, "Detecting spear-phishing attacks using machine learning," Ph.D. dissertation, Dublin, National College of Ireland, 2023.

[18] J. I. Fidelis, "Protection against spear phishing attacks using the ensemble method of machine learning," Ph.D. dissertation, Dublin, National College of Ireland, 2025.