Science Forum (Journal of Pure and Applied Sciences)

Journal Homepage: https://atbuscienceforum.com.ng/index.php/jpas

# An Integrated Framework for Combating Phishing in Nigeria's Midstream and Downstream Oil and Gas Operations

Ishaq Hassan[1], Muhammad Aminu Ahmed[1], Ahmed Abubakar Aliyu[1], Mohammed Ibrahim[1], Abubakar Muazu Ahmed[1], Sa'adatu Abdulkadir[1], Adamu Abdullahi[1] and Ibrahim Hassan[2]

[1] Faculty of Computing, Kaduna State University, Kaduna, Nigeria

[2] Department of Civil Engineering, Abubakar Tafawa Balewa University, Bauchi, Nigeria

## Abstract

In recent years, corporate organizations have increasingly adopted digital technologies to enhance their operations. However, this digital transformation has also heightened their exposure to cybersecurity threats—particularly phishing attacks. The Nigerian oil and gas sector, a critical component of the national economy, is particularly vulnerable, with frequent phishing incidents targeting sensitive corporate data and operational stability. Despite the adoption of mitigation measures such as employee training and email filtering, phishing remains a persistent threat, often exacerbated by human error and outdated systems. This paper proposes a comprehensive framework for mitigating phishing attacks within Nigeria's midstream and downstream oil and gas subsectors. The framework leverages ISO 27001 principles and incorporates a machine learning-based detection mechanism, specifically using a logistic regression model trained on localized enterprise data. It emphasizes continuous security risk assessment and integrates both technical controls and human-centric strategies. To validate the framework, interviews were conducted with industry stakeholders to assess current mitigation practices. The detection mechanism also utilizes data from Microsoft Defender alerts and the Anti-Phishing Working Group (APWG) repositories. The logistic regression model demonstrated a high accuracy rate of 97.7%, highlighting its effectiveness with minimal computational overhead. Findings further underscore the need for improved employee training, updated technical safeguards, and robust incident response plans to enhance cybersecurity resilience across the sector.

Keywords
Mitigating Phishing;
Nigeria;
Oil and Gas Industry;
Digital transformation

Corresponding Author: Ishaq Hassan, Faculty of Computing, Kaduna State University, Kaduna, Nigeria, Email ishaqme@live.co.uk 

## INTRODUCTION

The oil and gas sector is a cornerstone of Nigeria's economy, accounting for a substantial portion of the country's GDP, export revenue, and employment opportunities (Oguntoye, and Oguntoye 2021). The Nigerian oil and gas industry is comprised of upstream, midstream and downstream operations (Aniebo and Mogbo 2024). The upstream operations deal with the exploration and production of crude oil on both shores and offshore. The midstream operations on the other hand deal with the movement and processing/refining of the crude oil and terminal operations. Lastly, the downstream operations involve the storage, distribution and marketing operations of refined petroleum products (Aniebo and Mogbo 2024).

The Downstream, Midstream and Upstream subsectors of the Nigerian Oil and gas sector are regulated by different bodies which relies heavily on digital technologies for their operations. Nigerian Upstream Petroleum Regulatory Commission (NUPRC) regulates upstream operations, while Nigerian Midstream and Downstream Petroleum Regulatory Authority (NMDPRA) is the apex regulator of the Midstream and Downstream. The growing reliance digital infrastructure by these organizations necessitates the need to counter cybersecurity threats, particularly phishing attacks. (Akpan, 2024) noted that phishing attacks targeting Nigerian oil and gas companies have increased in sophistication and frequency, endangering both data security and business continuity.

Despite various cybersecurity initiatives, including firewalls, intrusion detection systems, and employee awareness programs, phishing remains a persistent threat (Anti-Phishing Working Group, 2019). According to Oest et al. (2019), the repercussions of successful phishing attacks can be severe, leading to financial losses, reputational damage, regulatory penalties, and disruption of essential services.

Recent research on phishing mitigation strategies underscores the need for tailored analytical frameworks and simulation models to comprehend and combat phishing threats more effectively. For instance, Kulkarni et al. (2024) proposed a general analytical framework that uses simulation models to identify and respond to phishing threats. While such frameworks provide a solid foundation, they do not account for the specific socio-economic and operational challenges prevalent in Nigeria's oil and gas industry. Moreover, existing literature often lacks empirical data specific to Nigeria, where socio-economic variables such as resource availability, regulatory constraints, and workforce capabilities present distinct challenges. These factors necessitate a customized approach to cybersecurity, as generic solutions may fail to address the sector's unique risk landscape. The industry's heavy reliance on third-party vendors, complex supply chains, and frequent cross-border data exchanges add further complexity to the cybersecurity requirements for Nigeria's midstream and downstream sectors (El Aassal et al., 2020).

This research proposes a framework specifically tailored to address phishing threats within Nigeria's midstream and downstream oil and gas sectors. Machine Learning techniques are employed and best practices from ISO 27001were adhered to.

The proposed framework seeks to enhance the resilience of Nigeria's oil and gas organizations against phishing threats, offering a practical approach to reducing vulnerabilities and strengthening overall security posture.

### 1.1 What is Phishing?

Phishing is a social engineering attack where an attacker tricks or manipulates individuals into revealing sensitive information, posing a direct threat to the confidentiality and operational integrity of organizations in this sector (Anilkumar et al., 2023). It can also be described as the fraudulent practice of stealing any person's confidential data, such as financial records, login credentials etc (Anilkumar et al., 2023).

According to Calder, (2020), globally recognized standards, such as ISO 27001 provide comprehensive guidelines for establishing and maintaining an information security management system (ISMS) that helps mitigate cybersecurity threats. ISO 27001's structured approach, which involves identifying risks, implementing controls, and monitoring security protocols, is essential for industries handling sensitive information. Studies, such as Shohoud (2023), demonstrate ISO 27001's effectiveness in cybersecurity threat mitigation. However, there is a notable gap in the application of these principles tailored specifically to the Nigerian oil and gas sector. According to Pascoe et al., (2024), the NIST Cyber security framework on the other hand provides organizations and industries of all sizes and sectors including government and academia with help on how to manage and reduce their risk of cyberattack. While the CSF provide a set of functions (Govern, Identify, Protect, Detect, Respond and Recover) to be used with other resources to better manage cybersecurity risks in organizations, it does not provide actionable strategies for how the outcomes should be achieved.

## 2. Phishing Detection & Mitigation Strategies

Phishing attacks manifest in different forms which range from email phishing to spear-phishing, whaling, vishing, and smishing (SMS phishing) according to Muntode and Parwe (2019). Human psychology along with technological vulnerabilities serve as the basis for phishing attacks that have become the most widespread cyber threat.

An increasing complexity in phishing attacks can be attributed to attackers who use artificial intelligence (AI) and machine learning (ML) together with social engineering tactics to boost their deception methods (Desetty, Jangampet & Pulyala, 2020). Sophisticated spoofing methods through domain impersonation and deepfake technology help modern phishing attacks evade detection because they originated from basic deceptive email schemes (Ali & Mohd Zaharon, 2024).

Advanced phishing techniques circumvent basic technical controls by using social engineering to deliver deceptive messages through technical controls because these techniques cannot guarantee full protection against new attacks (Bellamkonda, 2020). Organizations must adopt human-focused approaches because they prove crucial to fight phishing attacks. Organizations enhance their defense capabilities through employee education regarding phishing because staff

receive training that helps them detect potential attacks (Czuryk, 2023).

### 2.1 The ISO 27001 standard

The ISO 27001 provides requirements to establish, implement, maintain and continually improve an information security management system (ISO/IEC 27001, 2022). It proves adaptable for different industrial settings hence, it works well with the oil and gas sector that battles growing cybersecurity threats (El-Bably, 2021). Organizations need ISO 27001 as an international standard to implement its information security management system (ISMS) structure which protects sensitive business data. With its guidelines the standard provides organizations best practices which help them implement security controls and carrying out risk assessments and continuous monitoring activities to combat cybersecurity threats such as phishing (Ganji et al., 2019). Businesses which implement ISO 27001 create security policies that decrease phishing attack risks through their strict access control systems and protective data measures as well as their training programs for staff members (Šikman, Latinović & Paspalj, 2019).

## 3. Related Works

Anilkumar et al. (2023) highlighted the deceptive nature of phishing attacks that aim to trick users into divulging sensitive information. The methodology employed in the study involves a thorough survey of existing literature on phishing email detection techniques, with a particular focus on Natural Language Processing (NLP) methods. The authors explore various feature extraction and selection strategies that are essential for identifying spam content, categorizing features commonly used in phishing detection, and elucidating the mechanisms by which phishing attacks operate. Abahussain and Harrath (2019) pointed out that the increased usage of email has also made it a target for cybercriminals, necessitating effective strategies to combat malicious emails.

The methodology adopted in the study focuses on developing an optimal logical approach to filter out malicious emails, thereby reducing the likelihood of users falling victim to phishing and other email-based threats. They employ regular expressions and database techniques to identify and classify potentially harmful emails, aiming to enhance the security of email communications. Li, Zhang, and Wu (2020) argued that humans are often the weakest link in security, making them prime targets to phishing attacks. The methodology employed in this study introduces a novel detection approach grounded in the principles of persuasion.

The authors analyse the language used in phishing emails, focusing on specific words that may trigger a response from the reader. Utilizing an information gain algorithm, they select 25 key features relevant to detecting phishing attempts. The effectiveness of their method is empirically validated, achieving an impressive accuracy rate of 99.6%. Ragheb, Elmedany, and Sharif (2023) emphasized the critical importance of email security for organizations and explore two widely used frameworks: Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM), focusing on their effectiveness in authenticating emails. Through a comparative analysis, they conclude that while both

frameworks provide a level of protection against email threats, DKIM is superior due to its more comprehensive approach to authentication. Yu et al. (2022) conducted a thorough analysis of the email transmission process, identifying new techniques that can bypass established security protocols such as SPF and DMARC. Their large-scale experiments with prominent email service providers revealed vulnerabilities that could be exploited, highlighting the inadequacy of current protections against sophisticated spoofing methods. Imran et al. (2021) review synthesized existing research on both technical frameworks and non-technical approaches to risk management, highlighting the need for a holistic strategy that encompasses not only technological solutions but also human factors and organizational culture. Stergiopoulos, G., Gritzalis, D.A., and Limnaios, E. (2020) employed a qualitative methodology, analysing various incident reports and attack patterns specific to the oil and gas sector to assess the vulnerabilities and potential impacts of cyber-attacks. They identified key attack vectors and categorized incidents to provide a systematic understanding of the threat landscape.

Kulkarni, et al., (2024) delved into the complexities of email phishing, employing an analytical framework to dissect various tactics, including phishing, corporate email compromise, and email spoofing. Utilizing a combination of literature review, case studies of past incidents, and ethical considerations, the authors developed simulation models to test preventive measures against phishing attacks, employing tools like HiddenEye and Sendemail for controlled simulations. Shohoud, M. (2023) evaluated the role of the ISO 27001 standard as a proactive cybersecurity framework specifically for the downstream oil and gas sector in Egypt, which has faced increasing cyber threats alongside its digital transformation. The methodology includes surveys conducted on LinkedIn to gather professional insights on cybersecurity challenges and practices within the industry.

## 4. Methodology

In this section, the proposed framework for mitigating Phishing attacks is presented. In this work both qualitative and qualitative data were utilized. Interviews were conducted with industry stakeholders in the oil and gas sector in order to assess their experiences regarding phishing threats and identify specific vulnerabilities within their organizations. Dataset was equally used to train a machine learning model.

### 4.1 The existing Phishing Mitigation Strategies in the oil and gas sector

From our interview with an IT security manager and two IT support officers, the respondents described various measures that can be taken to minimize the impact of phishing attack, among which are employee training/awareness and implementation of network access controls. An IT support officer however, suggested newer measures which include, advanced email filtrations, bi-quarterly phishing simulation practices and multifactor authentications which he claimed has helped in minimizing formidable attacks.

### 4.2 The Proposed framework

The framework proposed in this work represents the overall strategy to prevent phishing attacks is shown in figure 1. The

framework operates as a system with modules designated for risk assessment and analysis, and prevention measures and detection. Results from risk assessment directly shape the development of usable strategies to be used as preventive measures. The detection module, which is an innovation and improvement over the existing practices, uses a machine learning algorithm trained on data harvested by the organization. The detection module seeks to alert or prompt admin on the possible occurrence of phishing attack.

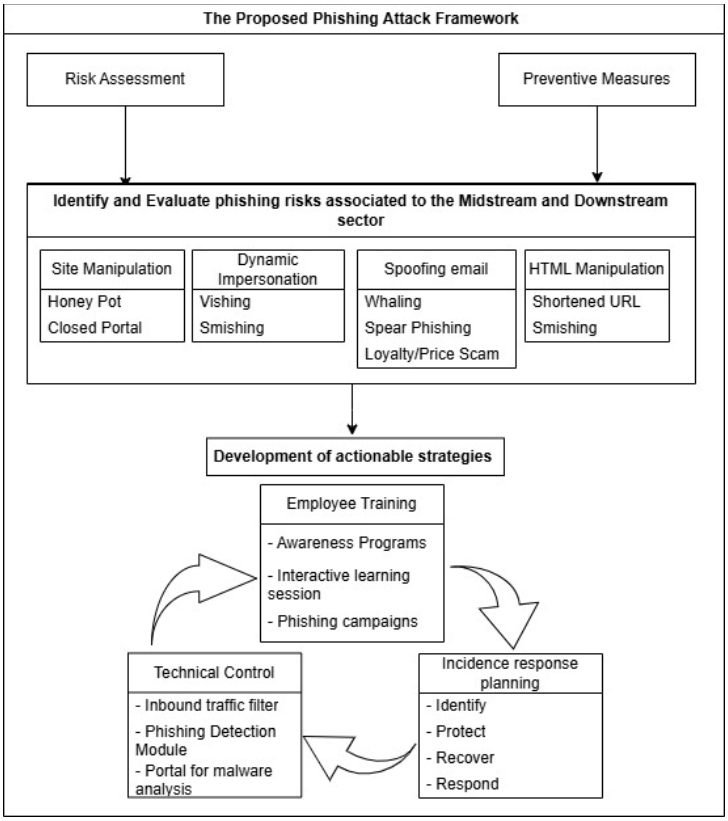



Figure 1. Proposed Framework for mitigating phishing

The framework features an iterative loop of the actionable strategies; namely, training of employees, implementation of technical controls, and development of incident response planning to enhance a concept of cyclic evolution.

Risk assessment identifies and analyses various threats, including phishing, vulnerabilities within system and the potential impact of these vulnerabilities on an organization. Site manipulation and dynamic impersonation as well as email spoofing and HTML manipulation are the attack vectors which require analysis during this phase. The defined attack types originate from interviews and surveys along with previous phishing incident examinations which create an

exhaustive mapping of sector vulnerabilities. A detailed evaluation of security risks enables deployment of proper preventive measures. The preventive measures component focuses on the creation of the necessary steps to avoid the identified risks and proper solutions or measures. Some of these measures include employee awareness and training, incidence response planning, and technical control.

The technical control aspect of the framework entails development of a module or tool that uses historical data to detect the possibility of phishing attack. To this end, logistic regression model was trained on the locally harvested data to detect phishing attack. Figure 2 depicts the work flow or pipeline for detecting phishing attacks using Machine Learning (ML) in Nigeria's midstream and downstream oil and gas sector.

It is important to state that incorporation of the machine learning based module as part of the technical control mechanism of the framework represents an enhancement over the existing phishing mitigation strategies currently employed in the sector.

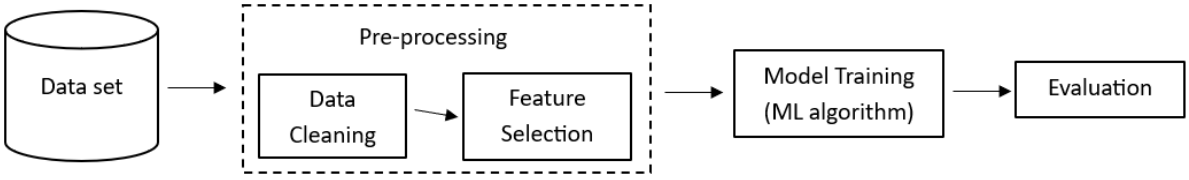



Figure 2: Workflow of the Phishing Attack detection

## 5. Implementation

This section basically explains the phishing detection module of the framework. The detection modules were implemented using python on google colab environment.

### 5.1 Data Pre-Processing

Qualitative data was obtained on request from the Nigerian Midstream and Downstream Petroleum Regulatory Authority (NMDPRA), from the data set "Alerts of Microsoft defender (June 2024–December 2024)." This dataset offers a range of cybersecurity events and possible phishing information from 29th June of 2024 to 22nd December 2024.

Data Cleaning: The dataset contains 2942 records. Duplicate entries were removed. Missing values were filled using forward-fill method. This process led to the reduction of the dataset to 441 records. The Cleaned Dataset Overview is presented in the figure 3. The data was converted and recoded into numerical forms for modelling. Fields including 'Alert name', 'Tags', 'Investigation state', 'Category', 'Detection source', 'Classification', and 'Determination' were performed using Label Encoding in order to make them compatible with the machine learning algorithm. The numerical columns like Incident Id and Active alerts were standardized in an effort to equalize/normalize the data in each column. The transformed data is shown in figure 3.

```
Columns in the Dataset: ['Alert name', 'Tags', 'Severity', 'Investigation state', 'Status', 'Category', 'Detection source', 'Impacted assets', 'First activity', 'Last activity

No numerical columns found for scaling. Skipping normalization.

Categorical Columns Found: ['Alert name', 'Tags', 'Investigation state', 'Category', 'Detection source', 'Classification', 'Determination', 'Assigned to']

Transformed Dataset Overview:
    Alert name  Tags Severity  Investigation state      Status  Category  \
6           32     0     High                    0    Resolved         0
10          37     0     High                    0    Resolved         3
21          33     0     High                    0         New         2
23          36     1     High                    1         New         4
24          12     0     High                    8  InProgress         7


Transformed Dataset Information:
<class 'pandas.core.frame.DataFrame'>
Index: 441 entries, 6 to 2926
Data columns (total 14 columns):
 #   Column               Non-Null Count  Dtype
---  ------               --------------  -----
 0   Alert name           441 non-null    int64
 1   Tags                 441 non-null    int64
 2   Severity             441 non-null    object
 3   Investigation state  441 non-null    int64
 4   Status               441 non-null    object
 5   Category             441 non-null    int64
 6   Detection source     441 non-null    int64
 7   Impacted assets      441 non-null    object
 8   First activity       441 non-null    object
 9   Last activity        441 non-null    object
 10  Policy name          0 non-null      float64
 11  Classification       441 non-null    int64
 12  Determination        441 non-null    int64
 13  Assigned to          441 non-null    int64
dtypes: float64(1), int64(8), object(5)
memory usage: 51.7+ KB
None
```

Figure 3: The transformed data

Feature selection: A correlation matrix serves as the first methodology to detect strongly linked features so that duplicative characteristics get eliminated from the data. Selecting unique informative features through feature selection leads to better model performance together with overfitting resistance. The chi-square test operates as a second technical tool to evaluate the statistical dependencies between target variable categories and value categories. The selection process for significant categorical variables occurs through chi-square score-based ranking which unveils the key predictors. The model training process utilizes recursive feature elimination (RFE) to systematically remove less significant attributes until it maintains only essential features that optimize performance and efficiency simultaneously.

In line with the principle of machine learning, the data set was split for training and testing respectively. 352 for the training while 89 for the test.

## 6. Evaluation

The evaluation of logistic regression model performance for its two-category data classification was carried out through confusion matrix analysis which reveals its accuracy in making correct instance category assignments. The matrix enables analysis to determine whether the model produces too many incorrect false positives for one class or incorrect false negatives for another class. The key metrics used are **Accuracy**, **Precision**, **Recall**, and **F1 Score**. These metrics ensure the robustness, reliability, and effectiveness of the phishing detection model.

i. **Accuracy:** The percentage of correctly identified phishing attempts versus total attempts.

$$Accuracy = \frac{True\ Positive+True\ Negative}{Total\ Sample} \quad (1)$$

ii. **Precision:** The ratio of true positive results to the total predicted positives.

$$\text{Precision} = \frac{True\ Positive}{True\ Positive+False\ Positive} \quad (2)$$

iii. **Recall:** The ratio of true positive results to the total actual positives.

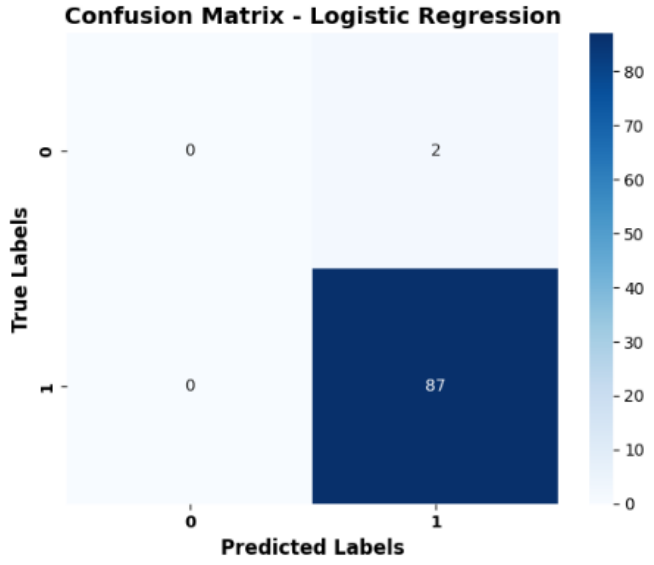
$$\text{Recall} = \frac{True\ Positive}{True\ Positives+False\ Negatives} \quad (3)$$

iv. **F1 Score:** The harmonic mean of precision and recall, providing a balance between the two metrics.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (4)$$

## 7. Results & Discussion

The confusion matrix of the logistic regression model is shown in figure 4. In the matrix, the first top-left cell represents true negatives and the top-right cell shows false positives while false negatives appear in the bottom-left and true positives are located in the bottom-right cell. The True Negative (TN) count consists of zero instances displayed in the cell at position (0,0). The model failed to classify any cases as belonging to the zero category. Two cases identified as class 1 turned out to be class 0 instances thus producing a total of 2 False Positives (FPs) according to the (0,1) cell. The False Negative (FN) count contains zero instances in the bottom-left cell (1,0) because the model did not mistake any samples as positive class 1. There were 87 positive instances which the model correctly identified as belonging to class 1 in the bottom-right cell (1,1).



The predictions from the model were correct in 97.7% of instances as indicated by its accuracy score. The precision value of 0.955 expresses how 95.5% of instances classified as class 1 actually belonged to that category. The recall value measures 1.0 indicating perfect detection of all actual positive outcomes. The F1-score reaches 0.966 which validates the model's high-quality performance across all metrics. The Logistic Regression model demonstrates strong performance according to the confusion matrix because it accurately identifies all instances as class 1 without any incorrect readings. Some incorrect predictions indicate the model tends to estimate the positive class (1) more frequently than expected. The model shows effective performance when classifying behavior due to its good accuracy level. The above results are summarized in tabular form shown in table 1.

Table 1: Performance Metrics of Logistic Regression Model

| Metric | Logistic Regression |
|---|---|
| Accuracy | 0.9775 |
| Precision | 0.9556 |
| Recall | 0.9775 |
| F1 Score | 0.9664 |

Table 1 shows the performance metrics for the Logistic Regression model showing key evaluation metrics that reflect the model's ability to make accurate predictions. The **accuracy** indicating that the model predicted the labels for 97.75% of the data. The **precision** shows that when the model predicts the positive class, it is correct 95.56% of the time. The **recall** showing that the model successfully identifies 97.75% of all actual positive instances. While the **F1 score** which is the harmonic mean of precision and recall, indicating a good balance between both metrics.

**The key findings:** Insights that could be derived from this work includes: Employee training proves crucial because it stands as the fundamental factor that strengthens corporate cyber security and minimizes security vulnerabilities from employee actions. Integration of machine learning based technique into the framework fit in nicely and does not results in overhead computationally, and ultimately enhances the framework's effectiveness.

## 8. Summary & Conclusion

In this paper, a framework for mitigating phishing attack in the Nigeria's midstream and downstream oil and gas sectors is presented. The framework is based on the principles of ISO 27001, tailored to the specific socio-economic context of Nigeria's oil and gas sector. Key components of the framework will include Risk Assessment – identify and evaluate phishing risks unique to the midstream and downstream sectors. Preventive Measures – develop actionable strategies to mitigate identified risks, including employee training, technical controls, and incident response planning. Detection

mechanism – train a machine learning model (logistic regression) on the enterprise data to detect phishing related attack. The incorporation of machine learning based detection module in the framework enhances the framework's ability to promptly alert or notify admin for immediate action to be taken. The performance of the logistic regression model in the framework reinforces the fact that embedding machine learning based techniques into software tools or frameworks can improve their effectiveness.

**References**

Abahussain, O., & Harrath, Y. (2019, September). Detection of malicious emails through regular expressions and databases. In *2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)* (pp. 1-5). IEEE. DOI: 10.1109/3ICT.2019.8910291

Akpan, U. E. (2024). Cybersecurity in the Petroleum Industry: A Comprehensive Review of Threats and Mitigation Strategies. Journal of Engineering Research and Reports, 26(12), 261-270.

Ali, M. M., & Mohd Zaharon, N. F. (2024). Phishing—A cyber fraud: The types, implications and governance. *International Journal of Educational Reform, 33(1)*, 101-121.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060. https://doi.org/10.3389/fcomp.2021.563060

Anilkumar, C., Karrothu, A., Mouli, N. S., & Tej, C. B. (2023, January). Recognition and processing of phishing emails using NLP: A survey. In *2023 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-4). IEEE.

Aniebo, I. N., & Mogbo, O. (2024). Energy Economics of Midstream and Downstream Petroleum Sectors in Nigeria: A Review of Potential Optimizations. SPE Nigeria Annual International Conference and Exhibition.

APWG, A. (2019). Phishing Activity Trends Report Q4 2018. *Comput. Fraud Secur*, *2019*, 4.

Bellamkonda, S. (2020). Cybersecurity in critical infrastructure: Protecting the foundations of modern society. International Journal of Communication Networks and Information Security, 12, 273-280.

Bhardwaj, A., Al-Turjman, F., Sapra, V., Kumar, M., & Stephan, T. (2021). Privacy-aware detection framework to mitigate new-age phishing attacks. *Computers & Electrical Engineering*, *96*, 107546. doi.org/10.1016/j.compeleceng.2021.107546.

Calder, A. (2020). Information Security based on ISO 27001/ISO 27002. Van Haren.

Czuryk, M. (2023). Cybersecurity and Protection of Critical Infrastructure. Studia Iuridica Lublinensia, 32(5), 43-52.

Desetty, A. G., Jangampet, V. D., & Pulyala, S. R. (2020). Phishing attacks: Evolving techniques, emerging trends, and countermeasure strategies. *International Journal for Innovative Engineering and Management Research*, *9*(12), 985-991.

Ebelogu, C. U., Prasad, R., Bisallah, H. I., Hammawa, B. M., & Musa, I. (2025). Investigation of Cybersecurity Vulnerabilities and Mitigation Strategies in Nigeria's Oil and Gas Industry. *ABUAD Journal of Engineering Research and Development (AJERD)*, *8*(1), 140-150. doi.org/10.53982/ajerd

El Aassal, A., Baki, S., Das, A., & Verma, R. M. (2020). An in-depth benchmarking and evaluation of phishing detection research for security needs. *Ieee Access*, *8*, 22170-22192. DOI: 10.1109/ICCCI56745.2023.10128481

El-Bably, A. Y. (2021). Overview of the impact of human error on cybersecurity based on ISO/IEC 27001 information security management. *Journal of Information Security and Cybercrimes Research, 4(1)*, 95-102.

Hands, A. S. (2022). Integrating quantitative and qualitative data in mixed methods research: An illustration. *The Canadian Journal of Information and Library Science*, *45*(1), 1-20. DOI: 10.5206/cjilsrcsib.v45i1.10645

Imran, H., Salama, M., Turner, C., & Fattah, S. (2021). A systematic literature review on the technical and non-technical cyber risk management models in the oil and gas sector. *Economic and Social Development: Book of Proceedings*, 218-234. DOI: 10.1007/978-3-030-98015-3_59

Kulkarni, M., Kumar, S., Panjwani, Y., Moharir, M., Kumar, A. A., & Baskaran, E. (2024, April). Mitigating Email Phishing: Analytical Framework, Simulation Models, and Preventive Measures. In *2024 10th International Conference on Communication and Signal Processing (ICCSP)* (pp. 1459-1464). IEEE. DOI: 10.1109/ICCSP60870.2024.10543325

Kushta, E., & Trushaj, G. (2020). Implementation of the Logistic Regression Model and Its Applications. *Journal of Advances in Mathematics*, *18*, 46-51. DOI: 10.24297/jam.v18i.8557

Li, X., Zhang, D., & Wu, B. (2020, June). Detection method of phishing email based on persuasion principle. In *2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)* (Vol. 1, pp. 571-574). IEEE. DOI: 10.1109/ITNEC48623.2020.9084766.

Marshall, N., Sturman, D., & Auton, J. C. (2023). Exploring the evidence for email phishing training: A scoping

review. *Computers & Security*, 103695. DOI: 10.1016/j.cose.2023.103695

Mohammed, A. S., Reinecke, P., Burnap, P., Rana, O., & Anthi, E. (2022). Cybersecurity challenges in the offshore oil and gas industry: an industrial cyber-physical systems (ICPS) perspective. *ACM Transactions on Cyber-Physical Systems (TCPS)*, *6*(3), 1-27. DOI:10.48550/arXiv.2202.12179

Muntode, A. R., & Parwe, S. S. (2019). An Overview on Phishing-its types and Countermeasures. International Journal of Engineering Research and, 8(12), 545-548.

Oest, A., Safaei, Y., Doupé, A., Ahn, G. J., Wardman, B., & Tyers, K. (2019, May). Phishfarm: A scalable framework for measuring the effectiveness of evasion techniques against browser phishing blacklists. In *2019 IEEE Symposium on Security and Privacy (SP)* (pp. 1344-1361). IEEE. DOI: 10.1109/SP.2019.00049.

Oguntoye, M., & Oguntoye, A. (2021). An appraisal of the impact of the oil sector on the Nigerian economy. *LLM Thesis Faculty of Law University of Lagos*.

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://doi.org/10.6028/NIST.CSWP.29

Ragheb, M. S., Elmedany, W., & Sharif, M. S. (2023, August). The effectiveness of dkim and spf in strengthening email security. In *2023 10th International Conference on Future Internet of Things and Cloud (FiCloud)* (pp. 422-426). IEEE. DOI: 10.1109/FiCloud58648.2023.00068.

Shohoud, M. (2023). Study the Effectiveness of ISO 27001 to Mitigate the Cyber Security Threats in the Egyptian Downstream Oil and Gas Industry. *Journal of Information Security*, *14*(2), 152-180. DOI: 10.4236/jis.2023.142010

Stergiopoulos, G., Gritzalis, D. A., & Limnaios, E. (2020). Cyber-attacks on the Oil & Gas sector: A survey on incident assessment and attack patterns. *Ieee Access*, *8*, 128440-128475. DOI: 10.1109/ACCESS.2020.3007960

Yu, B., Li, P., Liu, J., Zhou, Z., Han, Y., & Li, Z. (2022, June). Advanced analysis of email sender spoofing attack and related security problems. In *2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud (EdgeCom)* (pp. 80-85). IEEE. DOI: 10.1109/CSCloud-EdgeCom54986.2022.00023