International Journal of Science Academic Research
Vol. 05, Issue 09, pp.8287-8292, September, 2024
Available online at http://www.scienceijsar.com
ISSN: 2582-6425

Research Article

PREDICTION OF PHISHING ATTACKS IN ODL USING MACHINE LEARNING TECHNIQUES

[1, *]Garki, Farida Shehu, [2]Ogwueleka, Nonyelum Francisca and [3]Abdullahi, Fatimah Binta

[1]Department of Computer Science, National Open University of Nigeria
[2]Department of Computer Science, University of Abuja, Abuja, Nigeria

Received 14th July 2024; **Accepted** 20th August 2024; **Published online** 30th September 2024

Abstract

This study explores the growing reliance on e-learning platforms within Open and Distance Learning (ODL) institutions and the associated security challenges, particularly those related to social engineering. Social engineering, often referred to as human hacking, poses significant risks to the security and privacy of users by exploiting human factors rather than technical vulnerabilities. While traditional security measures like firewalls and encryption focus on technical defenses, they often fall short in mitigating these human-centered attacks. The research aims to address this gap by proposing a machine-learning approach to detect social engineering vulnerabilities in e-learning platforms. The study employs simulations to collect data, ensuring a comprehensive understanding of user behaviors and potential vulnerabilities. The data is processed, cleaned, and analyzed using various machine learning techniques, Random Forest, Decision Tree, and Recurrent Neural Network (RNN) are used to build the model. Evaluation of these models reveals that while the RNN model achieves the highest accuracy and precision, the Random Forest model offers the best balance across all metrics, making it a strong candidate for practical application. The findings underscore the importance of integrating targeted security measures to enhance the cybersecurity resilience of e-learning platforms. Through bridging theoretical insights with empirical testing, this study provides a practical solution to safeguarding e-learning systems from social engineering threats, emphasizing the need for ongoing awareness and proactive defense strategies.

Keywords: Social Engineering, E-learning, Vulnerabilities, Machine Learning, Cybersecurity.

INTRODUCTION

Computer networking has become integral to our daily lives (Singh *et al.,* 2022). This development birthed a system of learning that is widely known as e-learning (Harasim, 2006). This broadened the scope of the Open and Distance Learning (ODL) institutions (Paul & Tait, 2019), which started centuries ago as a correspondent system of learning. ODL has garnered a substantial increase in popularity in recent years, due to its advantages for people with hectic schedules or restricted access to conventional educational institutions (Tunstall, 2024). It is distinguished by the instructor's isolation from the student, with communication mostly mediated by technology (Bhebhe& Maphosa, 2020). The National Open University of Nigeria is the only institution in Nigeria (NOUN) that fully runs ODL (Agbu *et al.,* 2016). However, the heightened dependence on e-learning also brings forth fresh security issues. As more information is gathered and shared, protecting this information is becoming a concern, notably in connection to social engineering assaults (Bruma, 2020). Social engineering, also known as human hacking, is the art of tricking employees and consumers into disclosing their credentials and then using them to gain access to networks or accounts (Conteh & Schmick 2021). Social engineering vulnerabilities can expose sensitive data, compromise user accounts, and disrupt the normal functioning of the platform. Chetioui (2022) identified that social engineering methods and techniques involve using the communication channel to gain access to credentials. To ensure the security and privacy of users' data in e-learning systems, it is crucial to identify and address social engineering vulnerabilities. Traditional security measures like firewalls and encryption primarily focus on technical aspects and may not adequately mitigate social engineering attacks that exploit human factors (Dupont & Holt, 2022). Against this backdrop, this study proposes a machine-learning technique for detecting social engineering vulnerabilities in e-learning platforms.

LITERATURE REVIEW

Albladi & Weir (2020) established a conceptual model capable of assessing elements that affect users' assessment of social engineering-based assaults on social network sites.

Conteh & Schmick (2021) discuss the impact of social engineering, and its involvement in network breaches and cybercrime, and suggest defenses against such attacks.

Dhull (2016) compared and contrasted social engineering strategies by utilizing seven distinct characteristics, including time consumption, information delivered, role-playing, attack intensity, efficacy, targeted/untargeted, and direct/mediated.

Odeh *et al.* (2021) outlined the fundamental ideas behind social engineering assaults, the stages of execution, classifications, and kinds of these attacks, as well as strategies and tactics for minimizing them.

Almutairi (2022) through a survey found out knowledge gap in social engineering, out of 63.4% of the sample polled did not know about social engineering, 67.3% of the total samples were unaware of the risks posed by social engineering. Only 7.5% of the sample had good knowledge of social engineering, while 42.1% had only fair knowledge. In the same vein, Alharthi and Regan (2021) found that 45% of employees falsely believed they were not a target of cyberattacks. 84% of the participants overestimated the level of security on their work PCs.

Corresponding Author:** ***Garki, Farida Shehu,
Department of Computer Science, National Open University of Nigeria.

Yasin *et al.* (2021) developed an analytical methodology for social engineering assaults utilizing real-world situations in their paper titled Understanding and Decoding Social Engineering Attack Scenarios. Similarly, Quinlan (2020) suggested a defense against social engineering attacks for businesses based on a compilation of research into a model known as the SEDM. A model presented by Cletus (2018) was converted into a web application system that can recognize people susceptible to social engineering attempts. Alghenaim *et al.* (2021) created an employee awareness model to raise awareness of social engineering threats in the Saudi public sector.

Nguyen and Bhatia (2020) conducted a study aimed at devising a model to tackle social engineering attacks within higher education institutions. They examined different scenarios of social engineering attacks and put forth an awareness and training model to counter these threats effectively. However, the study's limitations included a reliance on theoretical constructs and a potential lack of real-world validation of the proposed model.

Grassegger and Nedbal's 2021 research investigated how employees' awareness of information security influences their inclination to resist social engineering. They conducted surveys among employees from diverse sectors to measure their information security awareness and their resistance intentions towards social engineering tactics. Statistical analyses were employed to explore the correlation between these factors. Nonetheless, the study had limitations, including potential biases due to reliance on self-reported data.

Literature on social engineering shows several research gaps, which form the basis of this dissertation. The existing studies are largely exploratory and theoretical, lacking empirical evidence and practical solutions for mitigating social engineering attacks. They focus on types of social engineering and epistemological concerns without testing the reliability of proposed models or their robustness in real-life scenarios. Mitigation strategies are discussed but not empirically validated. The human factor in social engineering is inadequately addressed, and scenario-based experiments fall short of real-world applicability. This study will bridge these gaps, by presenting empirical testing of mitigation strategies, validation of models, practical implementation of mitigation measures, bridging theoretical findings with practical applications, incorporating the human factor, and conducting real-world tests to ensure the effectiveness and practicality of proposed solutions.

MATERIALS AND METHODS

The research methodology outlined in Figure 1 begins with the problem definition, which focuses on predicting social engineering vulnerabilities in ODL. The next phase involves two primary methods: surveys and simulations. Surveys are used to gather responses from participants, potentially to understand their behavior, experiences, or attitudes related to social engineering. On the other hand, simulations are employed to create controlled environments or scenarios where data on vulnerabilities or responses to social engineering attacks can be collected. This dual approach allows for a comprehensive data collection process, capturing both real-world experiences and simulated outcomes. Once the data is collected, it undergoes data processing and cleaning. This step is essential for ensuring that the data is accurate, consistent, and free from errors or noise. With clean data in hand, the next step is quantitative analysis. This involves applying statistical or mathematical techniques to analyze the data and derive meaningful insights. Following the analysis, feature selection is performed to identify the most relevant variables or features in the dataset that are important for predicting vulnerabilities. Model selection follows feature selection, where appropriate machine learning models are chosen to predict vulnerabilities. Before the model is applied, the data is split into training and testing sets, typically with a 70/30 split. The trained model is then used to predict vulnerabilities based on the data provided. Model evaluation is performed next to assess the accuracy and reliability of the predictions. After the model has been validated, it is ready for implementation.

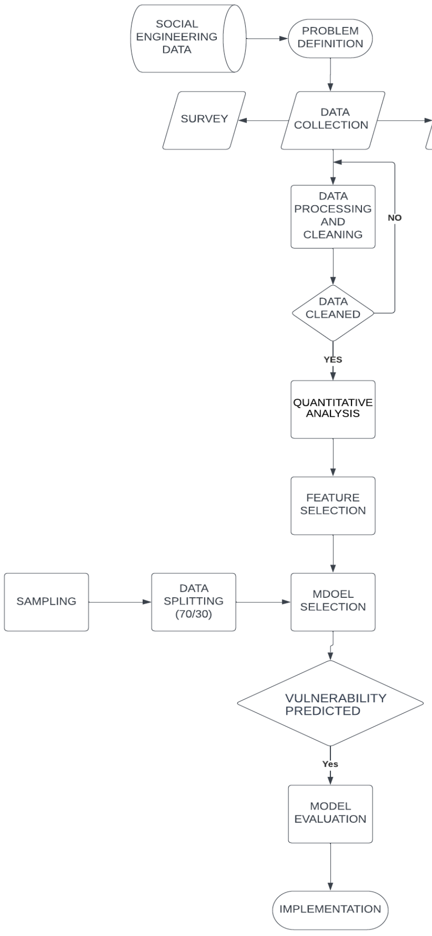
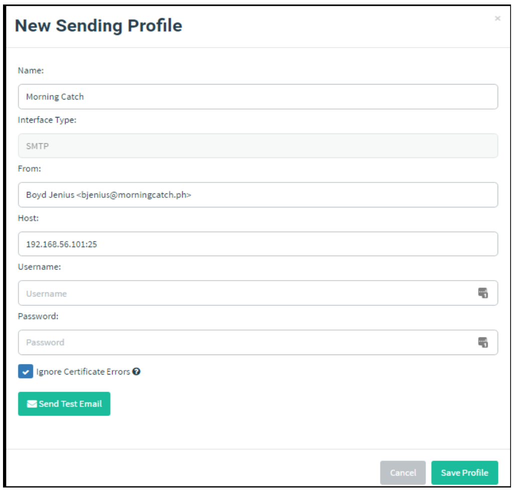


Figure 1. The Research Implementation

Data

The research collects data through simulated phishing assessments, which begin with the creation of realistic phishing scenarios. These scenarios are carefully crafted to resemble actual phishing tactics employed by cybercriminals. Scenarios include deceptive subject lines, enticing offers, and time-sensitive requests to elicit user engagement. A diverse group of participants, including employees from various departments, were randomly selected to ensure a representative sample with diverse levels of awareness. The distribution process is monitored and controlled to ensure participants know the purpose. The phishing campaign was then executed, the campaign aimed to gauge users' susceptibility to different tactics employed by attackers. Figure 2 - 6 shows the execution. The user actions are monitored and recorded with the simulated emails. This data helps identify individuals who were potentially exposed to phishing threats. Instances, where users provided sensitive information, such as login credentials or personal details, in response to the phishing emails,are documented. A record of users who reported the emails as suspicious is kept. Gophish's tracking and analysis features played a crucial role in monitoring user interactions in real time during the data collection. This includes tracking metrics such as opened emails, clicked links, and instances of submitted information. Gophish generated reports on click rates, providing information on the number of users who interacted with links. This metric helped assess the effectiveness of the simulated phishing emails in enticing users to take potentially harmful actions. Similarly, submission rates were tracked, shedding light on the success rates of social engineering tactics employed in the campaign. The platform is ideal for this study, because it facilitated timeline analysis, offering a detailed breakdown of user interactions over time. This analysis helped identify peak vulnerability periods and understand response times.



New Sending Profile

Name: Morning Catch

Interface Type: SMTP

From: Boyd Jenius <bjenius@morningcatch.ph>

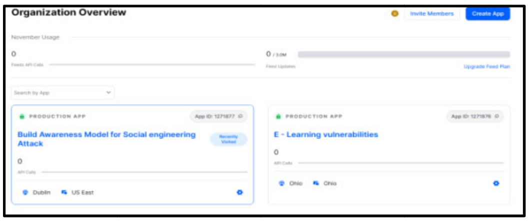
Host: 192.168.56.101:25

Username: Username

Password: Password

☑ Ignore Certificate Errors

Figure 2. The profile page of the phishing simulation platform



Organization Overview

November Usage

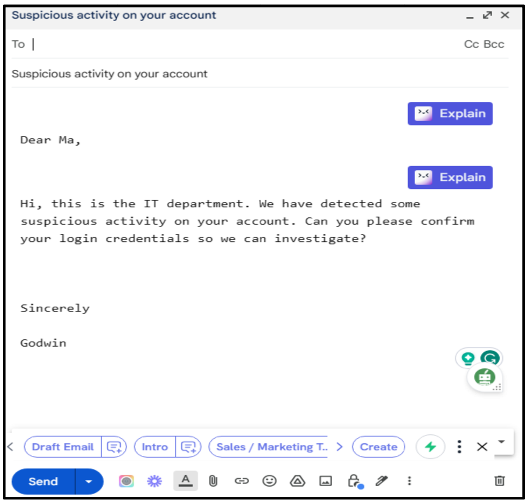
0 Feeds API Calls

0 / 3.0M Feed Updates

PRODUCTION APP App ID: 1271877 — Build Awareness Model for Social engineering Attack — 0 API Calls — Dublin, US East

PRODUCTION APP App ID: 1271876 — E - Learning vulnerabilities — 0 API Calls — Ohio, Ohio

Figure 3. Chat data builder



Suspicious activity on your account

To | Cc Bcc

Suspicious activity on your account

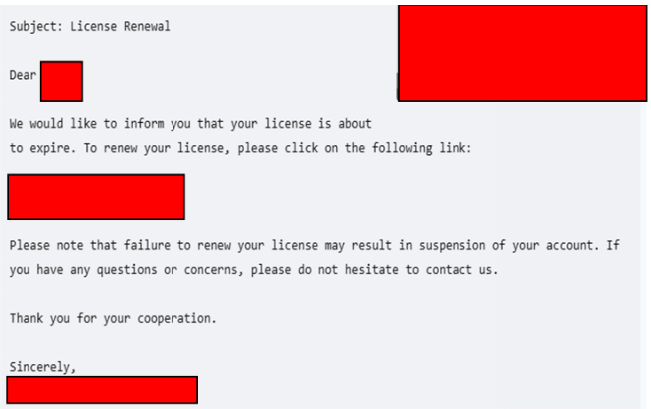
Dear Ma,

Hi, this is the IT department. We have detected some suspicious activity on your account. Can you please confirm your login credentials so we can investigate?

Sincerely

Godwin

Figure 4. An email sample prepared to be sent to users



Subject: License Renewal [redacted]

Dear [redacted]

We would like to inform you that your license is about to expire. To renew your license, please click on the following link:

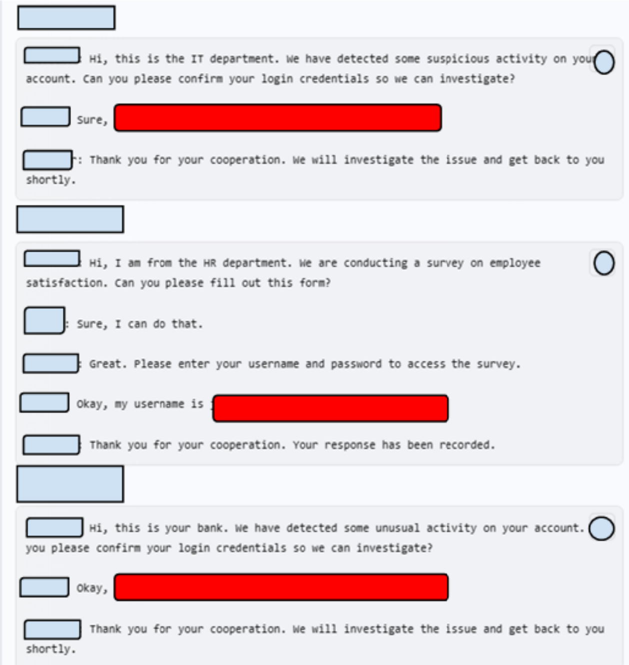
[redacted]

Please note that failure to renew your license may result in suspension of your account. If you have any questions or concerns, please do not hesitate to contact us.

Thank you for your cooperation.

Sincerely,
[redacted]

Figure 5. A Phishing Message



[redacted]

[redacted] Hi, this is the IT department. We have detected some suspicious activity on your account. Can you please confirm your login credentials so we can investigate?

[redacted] Sure, [redacted]

[redacted]: Thank you for your cooperation. We will investigate the issue and get back to you shortly.

[redacted]

[redacted] Hi, I am from the HR department. We are conducting a survey on employee satisfaction. Can you please fill out this form?

[redacted]: Sure, I can do that.

[redacted]: Great. Please enter your username and password to access the survey.

[redacted] Okay, my username is [redacted]

[redacted] Thank you for your cooperation. Your response has been recorded.

[redacted]

[redacted] Hi, this is your bank. We have detected some unusual activity on your account. you please confirm your login credentials so we can investigate?

[redacted] Okay, [redacted]

[redacted] Thank you for your cooperation. We will investigate the issue and get back to you shortly.

Figure 6. Samples of interactions with users

Data preparation was carried out on the text data which includes tokenization, stop word removal, and vectorization using Bag-of-Words (BoW) and TF-IDF techniques to represent each document as a vector of word frequencies. Check for missing values, duplicates, and inconsistent data type was carried out. The dataset underwent thorough preprocessing and cleaning. This preparation is to make the data fit for the machine learning procedures, ensuring accurate and reliable insights from the processed data. All columns were renamed to shorter names for easy access. To enable seamless integration with machine learning algorithms, all values were converted across all columns into numerical using nominal encoding. To mitigate imbalances in the dataset, particularly addressing the bias in classification, random oversampling is employed. Feature selection is employed to identify the most relevant features from the original dataset, thereby reducing dimensionality and complexity. Correlation, a statistical measure, plays a crucial role in this process by identifying features that have a significant relationship with the target variable and managing multicollinearity among features. In this study, features with high correlations with the target variable will be selected, and highly correlated pairs will be managed to avoid redundancy. Feature importance techniques complement correlation in selecting relevant features. These techniques assign scores to each feature based on their predictive value for the target variable. Tree-based method, Random Forest, is used to rank features by their contribution to model performance.

Model

The algorithms chosen in this study are based on their performance and popularity in predicting cyberattacks in literature. This study analyzes the use of these algorithms from literature, from which the most commonly used and effective ones, are chosen for this study. Two machine learning algorithms are chosen namely random forest and decision tree, and one deep learning algorithm Recurrent Neural Network (RNN) which is an implementation of the Artificial Neural Network (ANN). The rationale behind this is to test the robustness of these techniques in detecting phishing.

Model Training

The dataset was initially split into training and testing sets, with 80% of the data allocated for training and the remaining 20% for testing and validation. The training set was used to train and evaluate the selected algorithm, which proved to be successful in capturing the underlying patterns in the data. For the Recurrent Neural Network (RNN) model, a specific architecture was designed and implemented. The RNN model was constructed with a dense layer of 128 neurons using the ReLU activation function, followed by another dense layer with 64 neurons and the ReLU activation function. The final output layer consisted of a single neuron with a sigmoid activation function, suitable for binary classification tasks. The training process of the RNN involved 10 epochs.

Evaluation Metric

After training the machine learning model, its performance is evaluated. This evaluation uses metrics such as accuracy, precision, recall, and the F1-score to assess how effectively the model identifies social engineering threats and vulnerabilities.

Accuracy: Accuracy measures the ratio of correctly predicted instances to the total instances in the dataset.

Accuracy= (TP + TN) / (TP + TN + FP + FN) … 3.1

Precision (Positive Predictive Value): Precision measures the ratio of true positive predictions to all positive predictions made.

Precision = TP / (TP + FP) …. 3.2

Recall (Sensitivity, True Positive Rate): Recall measures the ratio of true positive predictions to all actual positives in the dataset.

Recall= TP / (TP + FN) ….. 3.3

F1-Score: The F1-Score is the harmonic mean of precision and recall. It balances precision and recall.

F1Score= 2*(Precision * Recall) / (Precision + Recall)…..3.4

Where:

TP = True positive
FN = False negative
TN = True negative
FP = False positive

RESULTS

The evaluation results of the three machine learning models Recurrent Neural Network (RNN), Decision Tree, and Random Forest presented in Figure 7 provide a comprehensive understanding of their performance across key metrics: Recall, F1 Score, Precision, and Accuracy. The recall score measures the ability of the models to identify true positives from all actual positive cases. The Random Forest model stands out with a recall score of 0.97, indicating its superior capability in detecting true positive cases. The Decision Tree follows closely with a recall score of 0.95, while the RNN model has the lowest recall at 0.89, suggesting it is less effective at capturing all true positives compared to the other models. When examining the F1 score, which balances both precision and recall, the Random Forest model again outperforms the others with a score of 0.97. This highlights its effectiveness in managing the trade-off between precision and recall, ensuring a good balance between identifying true positives and minimizing false positives. The Decision Tree model has an F1 score of 0.96, while the RNN model scores 0.94, indicating that while all models perform well, the Random Forest offers the best balance overall.

In terms of precision score, the RNN model achieves a perfect score of 1.0, meaning that all positive predictions made by this model are correct. However, this high precision is accompanied by a lower recall, indicating that the RNN might be missing some true positives in its predictions. The Random Forest and Decision Tree models also demonstrate high precision, with scores of 0.98 and 0.96, respectively, but they fall slightly short of the RNN's perfect precision. The accuracy score, which reflects the overall correctness of the model's predictions, shows that the RNN model is the most accurate, with a score of 0.98. The Random Forest model follows closely with an accuracy score of 0.97, while the Decision Tree lags with a score of 0.94. This suggests that, while the RNN is highly precise and accurate, the Random Forest model offers a more balanced performance across all metrics, making it a strong candidate for applications where both recall and precision are critical.

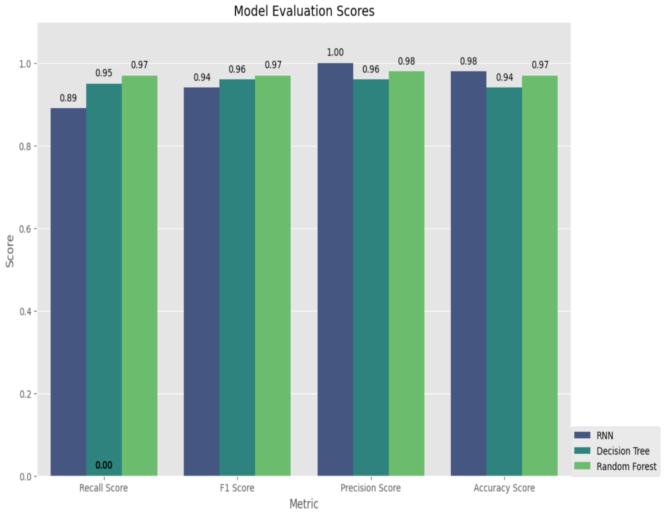


Figure 7. Model evaluation

DISCUSSION

The obtained results affirm the vulnerability of users to social engineering attacks and highlight the prevalence of techniques that pose a potential threat to the cybersecurity integrity of ODL. These findings emphasize the crucial need for targeted security measures and proactive strategies to bolster the overall cybersecurity resilience of the e-learning platform. The analysis conducted aligns with insights drawn from various studies on social engineering attacks. For instance, Albladi and Weir (2020) established a conceptual model to evaluate elements influencing users' perceptions of social engineering assaults, reflecting the need for a nuanced understanding of user behaviors. Dhull (2016) categorized social engineering strategies based on distinct characteristics, emphasizing factors such as time consumption and attack intensity, aligning with the approach of identifying patterns and potential threats in this analysis. Conteh & Schmick (2021) highlighted the significance of defenses against social engineering, a theme echoed in the identification of potential phishing attempts in the message content. Additionally, Yasin's (2021) analytical methodology for social engineering assaults, rooted in real-world scenarios, resonates with the identification of patterns in message content to uncover potential threats. The findings also correlate with studies addressing the lack of awareness among individuals regarding social engineering techniques. Almutairi's (2022) study in the educational sector and Alharthi and Regan's (2021) findings on employees overestimating security levels align with the identified need for improved awareness and understanding of potential risks in communication. Furthermore, the emphasis on proactive defenses and employee awareness models, as suggested by Quinlan (2020) and Alghenaim (2021) respectively, aligns with the theme of mitigating risks associated with social engineering. The analysis, through the identification of potential phishing indicators, contributes to the broader dialogue on practical approaches for preventing social engineering attacks. The study shows While models help in detection, educating users about phishing threats and safe practices is equally crucial. Incorporating phishing awareness programs within the eLearning platform can complement technical measures and enhance overall security. This approach will help balance the need for effective detection with the importance of maintaining a positive user experience. The study addresses the research gap by providing empirical evidence and practical solutions for mitigating social engineering attacks. Other than focusing on knowledge gaps, testing the reliability of proposed models or their robustness in real-life scenarios. Hence, this study bridges the gaps, by presenting empirical testing of mitigation strategies, validation of models, bridging theoretical findings with practical applications, incorporating the human factor, and conducting real-world tests to ensure the effectiveness and practicality of proposed solutions.

Conclusion

The study contributes valuable insights to the understanding of social engineering vulnerabilities in ODL systems. The recommendations derived from phishing simulations, and machine learning models offer actionable strategies for enhancing security measures. The success of the machine learning model in predicting vulnerabilities underscores the potential of advanced analytics in cybersecurity. As educational institutions increasingly rely on online platforms, the findings provide timely and practical recommendations for mitigating social engineering vulnerabilities, ensuring a secure digital learning environment. Future research may delve deeper into the evolving landscape of cybersecurity threats in the educational sector and explore adaptive security measures to address emerging challenges.

REFERENCES

Agbu, J. F., Mulder, F., De Vries, F., Tenebe, V., & Caine, A. (2016). The best of two openworlds at the National Open University of Nigeria. *Open Praxis,* 8(2), 111-121.

Albladi, S. M., & Weir, G. R. (2020). Predictingindividuals' vulnerability to socialengineering in social networks. *Cybersecurity*, 3(1),1-19. https://doi.org/10.1186/s42400-020-00047-5.

Alghenaim, M. F., Bakar, N. A. A., Yusoff, R. C. M., Hassan, N. H., &Sallehudin, H. (2021). Employee Awareness Model to Enhance Awareness of Social Engineering Threats inthe Saudi Public Sector. *In 2021 International Congress of Advanced Technology and Engineering (ICOTEN)* (pp. 1-6). IEEE.

Almutairi, B.S. and Alghamdi, A. (2022) The Role of Social Engineering in Cybersecurity and Its Impact. *Journal of Information Security,* 13, 363-379. https://doi.org/10.4236/jis.2022.134020

Bhebhe, S., & Maphosa, C. (2020). An exploration ofonline assessment in institutions of higherlearning. The Impact of COVID-19 On the International Education System, 172-183.

Bruma, L. M. (2020). An approach for informationsecurity risk assessment in cloudenvironments. *Informatica Economica,* 24(4), 29-40.

Chetioui, K., Bah, B., Alami, A. O., &Bahnasse, A. (2022). Overview of social engineeringattacks on social networks. *Procedia Computer Science,* 198, 656-661. https://doi.org/10.1016/j.procs.2021.12.302.

Cletus, A., & Najim, U (2018). Towards Securing Organizational Data against Social Engineering Attacks. *International Journal of Computer Applications,* 975, 8887.

Conteh, N. Y., & Schmick, P. J. (2021). Cybersecurityrisks, vulnerabilities, and countermeasures toprevent social engineering attacks. In Ethicalhacking techniques and counter measures for cybercrime prevention (pp. 19-31). IGI Global. DOI: https://doi.org/10.4018/978-1-7998-6504-9.ch002.

Dhull, R., & Hooda, S. S. (2016). Contrast Study of Social Engineering Techniques. *IOSR Journal of Computer Engineering,* 18(4), 66-68.

Dupont, B., & Holt, T. (2022). The Human Factor of Cybercrime. *Social Science Computer Review,* 40(4),860–864. https://doi.org/10.1177/08944393211011584

Grassegger, T., & Nedbal, D. (2021). The Role of Employees' Information Security Awarenesson the Intention to Resist Social Engineering. *Procedia Computer Science,* 181, 59-66. https://doi.org/10.1016/j.procs.2021.01.103

Harasim, L. (2006). A history of e-learning: Shifthappened. In The International Handbook of Virtual Learning Environments (pp. 59-94). Dordrecht: Springer Netherlands.

Nguyen, T., & Bhatia, S. (2020). Higher educationsocial engineering attack scenario, awareness & training model. *In Journal of The Colloquium for Information Systems Security Education* (Vol. 8, No. 1, pp. 8-8).

Odeh, N. A., Eleyan, D., Eleyan, A. (2021). A Surveyof Social Engineering Attacks: Detectionand Prevention Tools. *Journal of Theoretical and Applied Information Technology,* 99(18). ISSN: 1992-8645 www.jatit.org.

Paul, R., & Tait, A. (2019). Open universities: Past, present and future. *International Review of Research in Open and Distributed Learning,* 20(4), i-viii.

Quinlan, L. (2020). A Solution for Human Vulnerabilities to Social Engineering Attacks: *The Social Engineering Defence Model.* 10.13140/RG.2.2.35328.66562.

Singh, C. K., Pavithra, N., & Joshi, R. (2022). Internetan integral part of human life in 21st century: A review. *Current Journal of Applied Science and Technology,* 41(36), 12-18.

Tunstall, J. (Ed.). (2024). The open university opens. Taylor & Francis.

Yasin, A., Fatima, R., Liu, L., Wang, J., Ali, R., & Wei, Z. (2021). Understanding anddeciphering social engineering attackscenarios. *Security and Privacy,* 4(4), e161.

****