INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue V, May 2024

Phishing Attacks among Internet Banking Users in Nigeria: An Exploration of Remedial Strategies

Tepede Dipo

Babcock University, Nigeria

DOI : https://doi.org/10.51583/IJLTEMAS.2024.130512

Received: 30 April 2024; Accepted: 09 May 2024; Published: 11 June 2024

Abstract: This study meticulously examines phishing attacks targeting Nigerian internet banking users. It delves into prevailing trends, methodologies, and the effectiveness of existing countermeasures. It also proposes robust, tailored security measures in the form of a conceptual model. Similarly, by analyzing the latest tools and techniques, the study emphasizes the need for adaptive and continuously learning anti-phishing systems. The outcomes aim to empower stakeholders in the Nigerian banking sector, including policymakers, financial institutions, and users, to combat the complex and evolving threats posed by phishing attacks.

Keywords: Phishing attacks, Internet banking, Nigeria, Cybersecurity, Machine learning, Countermeasures, Adaptive systems, User awareness, Explainable AI, Behavioral Science, Economic impacts

I. Introduction

Phishing attacks relentlessly plague the cybersecurity landscape, deploying social engineering, exploiting vulnerabilities, and impersonating trusted brands to steal sensitive data [1]. This sophistication is on the rise, making detection a constant challenge [2].

To get a high-level comprehension of their processes, phishing attackers, often employ deceptive tactics by utilizing emails, fake websites, or social engineering, to exploit human vulnerabilities rather than technological flaws, posing a persistent and intricate challenge in cybersecurity [3]. These attacks have evolved to include highly targeted techniques like spear-phishing, vishing, and smishing, specifically targeting banking users and exploiting their trust in financial institutions [4].

Nigeria's 70 million active internet banking users, a prime target for cybercrime, suffered over 50% of cybercrime incidents in 2022 due to phishing, incurring billions in losses [5] [6].

Scholars point to the novelty of Internet banking, the surge in mobile banking, and low phishing awareness among Nigerians as root causes [7] [8]. Despite countermeasures, a critical gap remains in understanding and mitigating these evolving Nigerian-specific tactics [9].

This paper bridges this gap by meticulously analyzing prevailing trends and methodologies in Nigerian phishing attacks. It aims to propose tailored, robust security measures by unraveling their intricacies and discerning Nigerian patterns. These outcomes empower stakeholders to combat these evolving threats, significantly advancing cybersecurity in the Nigerian banking sector.

Also, this paper's outcome is anticipated to significantly contribute to cybersecurity in Nigerian Internet banking, providing strategic insights for financial institutions, policymakers, and users to strengthen their defenses against phishing attacks. By thoroughly evaluating the intricacies of these attacks and proposing customized defense mechanisms, this study seeks to empower stakeholders in the Nigerian banking sector to combat the pervasive threats posed by phishing attacks.

Furthermore, to adequately guide readers towards effectively consuming this paper, it has been problematized with the research question below

What are the latest tools and techniques utilized to detect and prevent phishing attacks on IB users in Nigeria?

How effective are existing and latest countermeasures against phishing attacks among IB users in Nigeria?

How, can we design effective phishing solutions and awareness programs for IB users in Nigeria?

II. Related Works

Addressing phishing attacks among Internet banking (IB) users in Nigeria remains a pertinent challenge, prompting a thorough exploration of the latest tools and techniques deployed for this purpose. Authors in [10] observed that among various attack vectors, websites stand out as the most popular target for phishing attempts. Attackers often replicate legitimate website pages and distribute deceptive URLs through spam messages, texts, or social media [11]. However, despite efforts to bolster website-based detection systems, concerns persist regarding their effectiveness, particularly due to limitations in feature selection methodologies [12]. In a similar vein, Balogun et al. [13] advocate the development of more effective feature engineering techniques for capturing the subtle nuances of phishing websites since the existing feature engineering methods often focus on extracting superficial features, making them less effective in distinguishing genuine websites from phishing attempts.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue V, May 2024

In response to evolving attack strategies, attempts to combat phishing through conventional means like URL blacklisting have proven insufficient in various contexts [14]. Also, researchers suggest innovative emerging solutions like automated whitelist-based detection systems [15]. Yet, while these systems demonstrate promising accuracy in controlled environments, their real-world applicability and performance on actual phishing websites remain untested and ambiguous [12] [15].

The efficacy of existing countermeasures against phishing attacks on IB users in Nigeria remains a subject of scrutiny. Machine learning (ML) emerges as a formidable contender in phishing detection, leveraging diverse website features for classification, thereby potentially identifying new phishing sites not yet blacklisted [16]. However, the impressive evaluations showcasing high accuracy (99.6%) and precision (99.2%) using large, balanced datasets [17] [12], often lack real-world dataset validation, potentially underestimating the true scope of phishing activities [18]. Criticisms against these evaluations highlight their potential lack of representation of evolving phishing trends.

Effectiveness hinges on the ability to distinguish genuine websites from phishing attempts. Scholars emphasize the need for diverse and realistic datasets to enhance model robustness and capture subtle differences between authentic and phishing websites in Nigeria [19] [13]. Additionally, the adaptability of current ML models to evolving attack techniques in the Nigerian context remains a concern, necessitating more resilient designs [12]. Using neuro-fuzzy approaches to combine the advantages of neural networks and fuzzy logic for phishing detection [20]. Neuro-fuzzy approaches can handle uncertainty and ambiguity in the data, and learn complex nonlinear relationships and rules for phishing detection. However, it requires a vast amount of labeled training data to learn and generalize accurately [21]. This is a significant obstacle, especially in the context of phishing, where new attack techniques emerge constantly. Also, it requires significant processing power and memory resources, hence computationally expensive to train.

To bolster ML anti-phishing solutions, researchers propose ensemble methods that amalgamate predictions from multiple algorithms, harnessing their strengths while mitigating weaknesses [19]. Also, out of the three classes of ensemble ML algorithms; bagging, boosting, and stacking, the author in [22] concludes that stacking is the best if the objective is to lower variance and bias and enhance overall performance. Furthermore, integrating the stacking ensemble method with other methods, such as meta-learning and cross-validation approaches may develop robust models like Support Vector Machine (SVM) and Naïve Bayes (NB) ensembles, showcase promising results but necessitate real-world validation [12]. Nevertheless, some authors argue that the stacking ensemble method requires more computational resources, is challenging to interpret the prediction process, and is susceptible to overfitting and sensitivity to hyperparameter tuning [23] [24].

Enhancing phishing solutions and awareness programs specifically tailored for IB users in Nigeria requires a nuanced approach. Deep learning (DL) algorithms exhibit potential superiority over ML counterparts, as evidenced by the exceptional performance of models like bidirectional encoder representations from transformers (BERT) and long short-term memory (LSTM) in phishing detection [25]. However, not all DL algorithms fare better, as demonstrated by Joshi et al. [26], highlighting the need for a nuanced comparison against other methodologies like Random Forest (RF) and Extreme Gradient Boost (XG Boost).

Explainable Artificial Intelligence (XAI) represents a burgeoning field within machine learning, aiming to demystify the inner workings of DL models, popularly labeled “black box”. The authors in [27] have contributed to this domain by devising an XAI-driven tool, leveraging Shapley Additive Explanations (SHAP), which serves as a valuable asset in model development, enabling in-depth exploration of misclassified instances. However, critiques from [28] and [29] center around several key aspects, such as interpretability from XAI doesn't guarantee a deep understanding of model decisions, lack of standardization in XAI methodologies leads to conflicting or varied explanations, XAI-generated explanations might be overly complex for non-technical users, and implementing XAI often increases the computational load, impacting performance, especially in resource-constrained scenarios.

Acknowledging technological advancements, researchers underscore the significance of end-user responsibility and targeted awareness campaigns to combat phishing attacks among IB users in Nigeria [30] [19]. In a divergent context, beyond simply sensitizing users about phishing attacks, some scholars are focused on a deeper understanding of the factors that contribute to the effectiveness of phishing attacks, including the role of social engineering techniques and the use of modern technologies [31] [32]. Consequently, this leads to deeper insights into psychological aspects of victim susceptibility and attacker motivations in the Nigerian context emerge as crucial areas for further research [33] [34].

For instance, the authors in [35] integrated two known psychological theories in technology avoidance behavior to develop a framework that can model phishing avoidance behavior among IB users in Nigeria. This anti-phishing solution takes into account the complex factors that influence user behavior to take a specific set of actions that protect themselves from phishing attacks. However, the authors in [36] argue that IB user behavior cannot be confidently predicted. Also, this technological avoidance behavior framework has not been empirically validated by the researchers. Furthermore, with over 90% of Nigerians identifying as Christians or Muslims [37], hence, any anti-phishing solution framework targeted at Nigerian IB users should go beyond relevant psychological theories to adopting and modeling religious ideals and idiosyncrasies.

Critically, evaluation methods for anti-phishing systems need to be rigorous [12] and warrant refinement to align with real-world scenarios in Nigeria, while discussions about the social and economic impacts of phishing among IB users in the country are currently underrepresented [31] [12]. Given the substantial financial implications of phishing, comprehensive assessments become imperative for effective anti-phishing strategies. In conclusion, addressing the evolving nature of phishing attacks on IB

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue V, May 2024

users in Nigeria necessitates adaptive and continuous learning approaches in detection systems [19]. Only through continual adaptation and learning from diverse and relevant data can these systems thwart the ever-evolving landscape of phishing threats in the Nigerian context.

III. Methodology

The methodology employed in this study involved an extensive review of literature sourced from prominent databases, including Research Gate, Science Direct, the ACM digital library, and the Springer database, recognized for their comprehensive coverage of computing [38]. The search criteria were confined to journal articles specifically associated with remedial solutions to phishing, focusing on publications between 2018 and 2023 to ensure relevance and currency.

A meticulous examination and analysis of these selected papers aimed to discern the gaps in anti-phishing solutions. These identified gaps served as foundational insights when formulating the steps within the conceptual model solution.

3.1 Ethical Consideration

Ethical considerations and treatment of data and participants should be prioritized to ensure the integrity and credibility of the study. Hence, ethical considerations may involve collecting, storing, and using sensitive information related to phishing incidents and countermeasures.

3.1.1 Informed Consent and Anonymity

Researchers must obtain informed consent from individual participants or organizations whose data may be analyzed, including their online behavior or personal information [39]. Additionally, researchers should ensure that all data presented in the study is anonymized to protect the privacy and confidentiality of the research participants [40]. Furthermore, proper citation practices should be followed to acknowledge the source of information [40].

3.1.2 Data Minimization and Secure Storage

Researchers should practice data minimization by collecting only the minimum amount of data necessary to achieve the research objectives [41]. Similarly, any collected data should be securely stored using encryption, access controls, and secure storage facilities or cloud services with robust security measures. Therefore, clear retention policies should be established to outline how long data will be retained and under what circumstances it will be securely disposed of

3.1.3 Research Purpose Transparency

Researchers should be transparent about how data will be used and ensure accountability for its proper handling [42]. This includes documenting data usage practices, adhering to ethical guidelines and regulations, and responding to inquiries or concerns from participants or regulatory authorities.

3.1.4 Cultural Sensitivity and Respect

Researchers should be mindful of cultural sensitivities and norms when conducting the study [43]. Also, practices or behaviors that may be considered taboo or offensive in certain cultural contexts should be avoided. Additionally, researchers should ensure that any awareness programs or interventions developed as part of the study are culturally sensitive and relevant to the Nigerian context.

IV. Findings

4.1 Tools and Techniques:

This section of the findings from the literature review adequately answers the first research question, “What are the latest tools and techniques utilized to detect and prevent phishing attacks on IB users in Nigeria?”

Website-based detection systems, despite efforts, their effectiveness remains limited due to feature selection limitations. However, automated whitelist-based detection systems demonstrate promising accuracy in controlled environments, but real-world applicability and performance need further investigation. Similarly, Neuro-fuzzy approaches offer advantages in handling uncertainty and ambiguity in data but require extensive data and computational resources.

Traditional ML models like Support Vector Machines (SVM) and Naïve Bayes (NB) show promising results, but lack real-world validation and require diverse datasets. To enhance traditional ML anti-phishing solutions, different Ensemble methods that combine strengths of multiple algorithms with stacking ensemble perform relatively better than other ensemble classification, but it requires significant resources and might suffer from overfitting. Notwithstanding, DL algorithms like BERT and LSTM exhibit potential superiority over traditional ML, but not all DL anti-phishing algorithms perform better than simpler models like RF and XG Boost. Finally, we can use Explainable AI (XAI) Tools like SHAP to interpret decisions that face limitations in standardization, user-friendliness, and computational complexity.

Other techniques include encouraging user responsibility through end-user awareness and targeted campaigns are crucial for combating phishing attacks. Also, understanding the psychological factors contributing to phishing effectiveness is essential for

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue V, May 2024

targeted interventions. Furthermore, anti-phishing solutions should be culturally sensitive and relevant to the Nigerian context especially integrating religious ideals and idiosyncrasies.

4.2 Effectiveness of Countermeasures:

The second research question, "How effective are existing and latest countermeasures against phishing attacks among IB users in Nigeria?", can be answered in this section of the findings.

Evaluations often showcase high accuracy on balanced datasets, potentially overestimating true performance in the field. Also, existing solutions struggle to adapt to the dynamic nature of phishing techniques. Furthermore, the lack of diverse and realistic datasets hinders model robustness and generalizability in capturing subtle phishing nuances.

In conclusion, there is limited consideration of social and economic impacts: Research often overlooks the broader consequences of phishing on IB users in Nigeria.

4.3 The Conceptual Model

The proposed conceptual model illustrated in Figure 1a encapsulates the findings from the various published texts to answer the final research question, "How can we design effective phishing solutions and awareness programs for IB users in Nigeria?"

Traditional ML is selected because it appears to be the most promising out of all the technology solutions offered in the evaluated literary texts since it has the potential to withstand evolving phishing attacks, requiring lower labeled datasets to train than its counterparts, such as DL and neuro-fuzzy solutions. Also, based on the selected ML option, it is easy to adapt and scale because it requires relatively less power and memory for computation. Furthermore, given its relatively high interpretability in decision-making, it has the potential to be a robust anti-phishing solution with the right configuration.

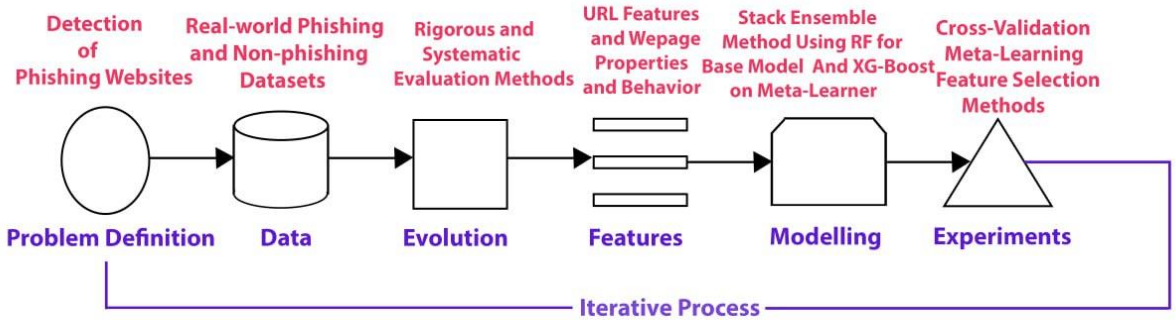

Figure 1a: Conceptual Robust Anti-phishing ML Solution for IB users in Nigeria (Bourke, 2019)

a. **Problem Definition:** Framing the existing anti-phishing problem among IB users in Nigeria into an ML problem is the first step in the proposed conceptual model. The first effective step is to detect phishing websites since websites appear to be the most popular attack vectors,

b. **Data:** The lack of diverse and realistic datasets hinders model robustness and generalizability in capturing subtle phishing nuances. Also, real-world dataset validation is often missing in evaluations, potentially underestimating the true scope of phishing activities. Hence, the need for data that reflects evolving phishing trends in the Nigerian context is crucial. The second step is to use real-time streaming data for training and testing.

c. **Evaluation:** Evaluations often showcase high accuracy but lack real-world validation, potentially overestimating model performance. Also, current evaluation methods lack rigor and need refinement to align with real-world scenarios. Hence, ML requires systematic and rigorous evaluation methods. The third step should focus on metrics, such as precision, recall, and AUC-ROC score, analyzing false positives and false negatives, and identifying key features to enhance interpretability.

d. **Features**: Existing feature engineering methods often focus on superficial features, making them less effective in phishing detection. Also, there is the need for more effective techniques to capture subtle nuances of phishing websites is highlighted. For instance, Orunsolu et al. [12]'s feature selection method uses an incremental component-based system

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue V, May 2024

to extract features from URLs, webpage properties, and webpage behavior. The fourth step is to select relevant features including website content, network traffic data, and user interaction data.

e. **Modeling**: The stacking ensemble is selected for its relative accuracy and precision. Random Forest (RF) is the base model because its bagging mechanism makes it prevents overfitting; it is relatively insensitive to outliers and missing values, making it suitable for handling diverse datasets often encountered in real-world applications; its interpretability is valuable for developing trust and confidence in the model, particularly in sensitive domains like financial services; its parallel processing allows for faster training and prediction, especially on large datasets; and its flexibility allows the model to be adapted to the specific characteristics of the base models and the meta-learner used in the stacking ensemble.

   XGBoost (eXtreme Gradient Boosting)'s combination of high accuracy, robust learning, efficient handling of large datasets, interpretability, flexible hyperparameters, and robustness to noise makes it a valuable choice for a meta-learner in ML stacking ensembles. This is why it is selected for the conceptual phishing detection model, where high accuracy and interpretability are crucial.

f. **Experiments**: Fine-tuning hyperparameters for optimal performance and robustness may include cross-validation, meta-learning, and investigating the impact of different features on model accuracy. The last step may include developing hybrid models combining different techniques and adapting models to evolve with changing phishing threats

4.3.1 Model Deployment and Awareness Programs:

For the conceptual model to perform effectively, it should be integrated into IB systems for real-time detection. The IB system should have user-friendly interfaces for reporting phishing attempts and for promoting responsible online behavior and vigilance.

Exploring the factors that influence user susceptibility to phishing attacks can inform targeted interventions. Also, ethical considerations regarding data collection, storage, and usage must be addressed.

Implementing awareness campaigns to educate users about phishing tactics and tailoring these programs to specific demographics and cultural contexts in Nigeria, especially exploration of religious ideals and idiosyncrasies.

4.3.2 Expected Outcomes:

We expect an increased detection rate and prevention of phishing attacks, reduced financial losses and data breaches, improved user confidence and security in online banking, and enhanced awareness and knowledge of phishing threats.

This conceptual model provides a framework for developing effective phishing solutions and awareness programs for IB users in Nigeria. By addressing the challenges and conducting further research, we can significantly improve the cybersecurity landscape and protect users from financial and data losses.

V. Conclusion

Combating phishing attacks on Internet banking (IB) users in Nigeria remains a critical challenge. Phishing attacks are a prevalent cybersecurity threat that poses significant financial and reputational risks. Researchers have proposed various mitigation strategies, including blacklists, whitelists, and machine learning (ML) approaches. However, these methods face challenges, such as the need for comprehensive datasets, robust feature engineering techniques, and adaptable algorithms. This article critically evaluates the effectiveness of these strategies and highlights the need for a more holistic approach that combines technology-based solutions with user education and a deeper understanding of phishing attacker motivations and tactics.

5.1 Limitations

While the paper provides an overview of phishing attacks on IB users in Nigeria, it has several limitations that should be considered:

Limited Scope: The paper focuses primarily on website-based detection systems since the website is the most popular vector [10]. Other common phishing vectors, such as email and social media, may require different detection and prevention strategies. Additionally, the paper focuses on technical solutions and does not explore the social and behavioral aspects of phishing susceptibility.

Data Sources: The paper relies heavily on existing research and lacks empirical data collected from Nigerian IB users. This limits the generalizability of the findings and the applicability of the proposed solutions to the Nigerian context.

Real-World Validation: Many of the reviewed anti-phishing solutions have not been validated in real-world settings. This raises questions about their effectiveness and ability to generalize to the diverse and dynamic landscape of phishing attacks.

Ethical Considerations: The paper mentions the need for ethical considerations regarding data collection and usage, but it does not provide a detailed discussion of potential ethical issues or how they can be addressed.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue V, May 2024

Impact on Users and Financial Institutions: The paper does not fully explore the social and economic impacts of phishing on IB users and financial institutions. This limits our understanding of the full extent of the problem and the potential benefits of implementing effective anti-phishing solutions**.**

Overall, these limitations suggest that further research and development are needed to fully understand and address the problem of phishing attacks on IB users in Nigeria. Future research should focus on collecting empirical data, developing and testing real-world solutions, and addressing the ethical and social implications of these solutions.

5.2 Recommendations:

This paper advises investment in research and development of adaptive and continuously learning anti-phishing systems. Cybersecurity scholars and stakeholders should prioritize real-world validation of proposed solutions to ensure effectiveness and generalizability. Financial institutions should promote responsible online behavior and vigilance among IB users through targeted awareness campaigns. They should develop culturally sensitive and context-aware phishing prevention strategies, such as religious ideals and idiosyncrasies. Also, cybersecurity scholars should integrate diverse data sources and utilize AI-powered tools for personalized risk assessment and mitigation.

There should be collaboration between researchers, financial institutions, and regulatory bodies to develop comprehensive anti-phishing frameworks. In conclusion, financial regulators should address data privacy and security concerns through ethical considerations and transparent data governance practices

5.3 Future Directions:

Scholars and practitioners should focus on the investigation of the social and economic impacts of phishing on IB users in Nigeria. They should explore the potential of AI-powered tools for personalized phishing prevention strategies and develop frameworks for integrating behavioral science and psychology into anti-phishing solutions. Also, they should conduct further research on explainable AI (XAI) techniques for interpreting model decisions and enhancing user trust. Furthermore, they should continuously adapt and evolve anti-phishing solutions to keep pace with the ever-changing phishing landscape.

In conclusion, effectively addressing phishing attacks in Nigeria requires a multi-pronged approach. Continuous research and development are needed to improve tools, techniques, and awareness programs. By addressing the limitations of existing solutions, prioritizing real-world validation, and considering the social and economic context, we can create a more secure environment for IB users in Nigeria.

References

1. Frontiers, “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy”, Dec. 2021, [Online]. Available: https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full
2. CNBC, “Phishing attacks are increasing and getting more sophisticated. Here's how to avoid them.”, Jan. 2023, [Online]. Available: https://www.cnbc.com/2023/01/07/phishing-attacks-are-increasing-and-getting-more-sophisticated.html
3. D. D. Dilrukshi, “Phishing Detection and Prevention Approaches: A Comprehensive Review”, IEEE Access, vol. 9, pp. 58465–58487, Dec. 2021.
4. M. D. Olarik and T. O. Olatayo, “An Empirical Study on Phishing Attacks and Countermeasures”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 4, no. 1, pp. 1–11, Dec. 2019.
5. CBN, “Annual Report and Statement of Accounts for the Year Ended 31st December 2022”, Dec. 2022.
6. Guardian Nigeria. “8.7% people in Nigeria, SSA suffer phishing in 2022.” Mar. 2022, [Online]. Available: https://guardian.ng/business-services/8-7-people-in-nigeria-ssa-suffer-phishing-in-2022/
7. A. Ashiru, “Identifying Phishing As A form of Cybercrime in Nigeria”, African Journal of University of Lagos, vol. 5, no. 1, pp. 178–189, Dec. 2023.
8. O. Oyebode, “Cybersecurity in Nigeria: A Review of the Legal Framework”, Journal of Cybersecurity and Privacy, vol. 1, no. 1, pp. 1–12, Dec. 2021.
9. A. N. Okafor, “Current Trends and Countermeasures of Phishing Attacks in Nigerian Banking Systems”, Journal of Cyber Security, vol. 3, no. 2, pp. 112–128, Dec. 2021.
10. B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedejiand J. Porras, “Mitigation strategies against the phishing attacks: A systematic literature review”, Computers & Security, vol. 132, p. 103387, Dec. 2023, doi: 10.1016/j.cose.2023.103387.
11. A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, “A comprehensive survey of AI-enabled phishing attacks detection techniques,” Telecommunication Systems, vol. 76, no. 1, Oct. 2020, doi: https://doi.org/10.1007/s11235-020-00733-2.
12. A. A. Orunsolu, A. S. Sodiya, and A. T. Akinwale, “A predictive model for phishing detection,” Journal of King Saud University - Computer and Information Sciences, Dec. 2019, doi: https://doi.org/10.1016/j.jksuci.2019.12.005.
13. A. O. Balogun et al., “Improving the phishing website detection using empirical analysis of Function Tree and its variants,” Heliyon, vol. 7, no. 7, p. e07437, Jul. 2021, doi: https://doi.org/10.1016/j.heliyon.2021.e07437.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue V, May 2024

14. S. H. Ahammad et al., "Phishing URL detection using machine learning methods," Advances in Engineering Software, vol. 173, p. 103288, Nov. 2022, doi: https://doi.org/10.1016/j.advengsoft.2022.103288.
15. N. Azeez, S. Misra, I. A. Margaret, L. Fernandez-Sanz, and S. M. Abdulhamid, "Adopting Automated Whitelist Approach for Detecting Phishing Attacks," Computers & Security, p. 102328, May 2021, doi: https://doi.org/10.1016/j.cose.2021.102328.
16. G. Harinahalli Lokesh and G. BoreGowda, "Phishing website detection based on effective machine learning approach," Journal of Cyber Security Technology, pp. 1–14, Aug. 2020, doi: https://doi.org/10.1080/23742917.2020.1813396.
17. M. Bahaghighat, M. Ghasemi, and F. Ozen, "A high-accuracy phishing website detection method based on machine learning," Journal of Information Security and Applications, vol. 77, p. 103553, Sep. 2023, doi: https://doi.org/10.1016/j.jisa.2023.103553.
18. R. Hoheisel, G. van Capelleveen, D. K. Sarmah, and M. Junger, "The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains," Computers & Security, vol. 128, p. 103158, May 2023, doi: https://doi.org/10.1016/j.cose.2023.103158.
19. T. O. Ojewumi, G. O. Ogunleye, B. O. Oguntunde, O. Folorunsho, S. G. Fashoto, and N. Ogbu, "Performance evaluation of machine learning tools for detection of phishing attacks on web pages," Scientific African, vol. 16, p. e01165, Jul. 2022, doi: https://doi.org/10.1016/j.sciaf.2022.e01165.
20. C. Pham, L. A. T. Nguyen, N. H. Tran, E.-N. Huh, and C. S. Hong, "Phishing-Aware: A Neuro-Fuzzy Approach for Anti-Phishing on Fog Networks," IEEE Transactions on Network and Service Management, vol. 15, no. 3, pp. 1076–1089, Sep. 2018, doi: https://doi.org/10.1109/tnsm.2018.2831197.
21. J. Yu, J. Li, Y. Liand Y. Wang, "A comparative study of machine learning techniques for phishing website detection", Journal of Network and Computer Applications, vol. 235, p. 107238, Dec. 2023.
22. E. Budu, "Bagging, Boosting, and Stacking in Machine Learning", Dec. 2023, [Online]. Available: https://www.baeldung.com/cs/bagging-boosting-stacking-ml-ensemble-models
23. X. Zhang and Z. Zhou, "On the drawbacks of stacking ensemble learning", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 45, no. 7, pp. 1610–1622, Dec. 2023, [Online]. Available: https://link.springer.com/article/10.1007/s10639-023-11682-z
24. J. Li, Y. Dengand Z. Tang, "Stacking ensemble learning: A critical review and comparative study", Journal of Machine Learning Research, vol. 24, no. 224, pp. 1–33, Dec. 2023, [Online]. Available: https://arxiv.org/abs/1407.1537
25. S. Atawneh and H. Aljehani, "Phishing Email Detection Model Using Deep Learning," Electronics, vol. 12, no. 20, p. 4261, Jan. 2023, doi: https://doi.org/10.3390/electronics12204261.
26. K. Joshi, C. Bhatt, K. Shah, D. Parmar, J. M. Corchado, A. Bruno, P. L. Mazzeo, "Machine-Learning Techniques for Predicting Phishing Attacks in Blockchain Networks: A Comparative Study," Algorithms, vol. 16, no. 8, pp. 366–366, Jul. 2023, doi: https://doi.org/10.3390/a16080366.
27. O. Ayoub, N. Di Cicco, F. Ezzeddine, F. Bruschetta, R. Rubino, M. Nardecchia, M. Milano, F. Musumeci, C. Passera, M. Tornatore, Explainable artificial intelligence in communication networks: a use case for failure identification in microwave networks, Comput. Netw. 219 (2022) 109466, https://doi.org/10.1016/j.comnet.2022.109466.
28. Z. C. Lipton, "The Mythos of Model Interpretability," Queue, vol. 16, no. 3, pp. 31–57, Jun. 2018, doi: https://doi.org/10.1145/3236386.3241340.
29. M. Benk and A. Ferrario, "Explaining Interpretable Machine Learning: Theory, Methods and Applications," SSRN Electronic Journal, 2020, Published, doi: 10.2139/ssrn.3748268.
30. G. Varshney, R. Kumawat, V. Varadharajan, U. Tupakula, and C. Gupta, "Anti-phishing: A comprehensive perspective," Expert Systems with Applications, vol. 238, p. 122199, Mar. 2024, doi: https://doi.org/10.1016/j.eswa.2023.122199.
31. P. N. Mangumt and K. A. Datukun, "The ever-changing face of phishing", World Journal of Innovative Research, vol. 10, no. 1, pp. 34–44, Dec. 2021.
32. M. Boddy, "Phishing 2.0: the new evolution in cybercrime", vol. 50, no. 10, pp. 8–13, Dec. 2018.
33. T. Xu, K. Singh, and P. Rajivan, "Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks," Applied Ergonomics, vol. 108, p. 103908, Apr. 2023, doi: https://doi.org/10.1016/j.apergo.2022.103908.
34. E. Tessian, "Tessian Spear-Phishing Threat Landscape 2021", Computer Fraud & Security, vol. 50, no. 10, pp. 8–13, Dec. 2021.
35. O. A. Fadare and M. A. Zahurin, "Modelling the phishing avoidance behaviour among internet banking users in Nigeria: The initial investigation", IAEME Journal of Computer Engineering and Technology, vol. 4, no. 1, pp. 1–17, Dec. 2020.
36. M. S. Kim and J. H. Kim, "Identifying user behavioral patterns in internet banking using deep learning-based sequential modeling", Journal of Information Processing Systems, vol. 19, no. 2, pp. 309–320, Dec. 2023.
37. A. O. Ayodeji and E. A. Adeniyi, "Religion and Sustainable Development in Nigeria: Issues and Prospects", Journal of Sustainable Development in Africa, vol. 19, no. 11, pp. 33–48, Dec. 2017.
38. A. Valente, M. Holanda, A. M. Mariano, R. Furutaand D. Da Silva, "Analysis of Academic Databases for Literature Review in the Computer Science Education Field", IEEE Frontiers in Education Conference (FIE), pp. 1–7, Dec. 2022.
39. G. Burkhardt, F. Boy, D. Doneddu, and N. Hajli, "Privacy Behaviour: A Model for Online Informed Consent," Journal of Business Ethics, vol. 186, no. 1, pp. 237–255, Jul. 2022, doi: 10.1007/s10551-022-05202-1.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue V, May 2024

40. K. Jane Smith, R. L. Michael, and T. C. Emily. "Ensuring Privacy and Confidentiality: Anonymization Techniques for Research Data". IEEE Transactions on Data Privacy, Volume 12, Issue 3, pages 123–138, 2022
41. L.J. Sarah, T.L. Mark, and R.C. Emily. "Data Minimization Strategies for Ethical Research: Balancing Objectives and Privacy". IEEE Transactions on Privacy and Security, Volume 9, Issue 2, pages 87–102, 2023
42. R. Williams et al., "From transparency to accountability of intelligent systems: Moving beyond aspirations," Data & Policy, vol. 4, 2022, doi: 10.1017/dap.2021.37.
43. K. Krys et al., "Introduction to a Culturally Sensitive Measure of Well-Being: Combining Life Satisfaction and Interdependent Happiness Across 49 Different Cultures," Journal of Happiness Studies, vol. 24, no. 2, pp. 607–627, Dec. 2022, doi: 10.1007/s10902-022-00588-1.