[10] Bahaghighat M., Ghasemi M., and Ozen F. (2023): A high-accuracy phishing website detection method based on machine learning, *Journal of Information Security and Applications*, Vol.77. https://doi.org/10.1016/j.jisa.2023.103553. Available: https://www.sciencedirect.com/science/article/pii/S2214212623001370 [Accessed September 7, 2023]
[11] Balogun A.O., et al. (2021), Improving the phishing website detection using empirical analysis of Function Tree and its variants. *Heliyon, Vol.* 7, No.7, June 2021. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8264617/ [Accessed September 7, 2023].
[12] Basit, A., *et al.* (2020, October 23). A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommunication Systems, 76(1), 139–154. https://doi.org/10.1007/s11235-020-00733-2
[13] Bharat, K., & Broder, A. (1998): A technique for measuring the relative size and overlap of public Web search engines. *Computer Networks*, 30(1–7), 107–117.
[14] Bourke D. (2019): A 6 Step Field Guide for Building Machine Learning Projects. [Online] Available: https://www.mrdbourke.com/a-6-step-field-guide-for-building-machine-learning-projects/ [Accessed September 7, 2023].
[15] Calzarossa M. C., Giudici P., and Zieni R. (2023): Explainable machine learning for phishing feature detection. Wiley. Available: DOI: 10.1002/qre.3411[Accessed September 7, 2023]
[16] Chen Y., Zhang Y., and Liu K., (2023): Factors affecting the success of machine learning models in real-world applications, *Machine Learning*, Vol.109, No.1, p.5-23.
[17] Chiew K.L., et al. (2019): A new hybrid ensemble feature selection framework for machine learning-based phishing detection system, *Inf. Sci*. 484 (2019) 153–166.
[18] Columbus, L. (2020): 5 Ways ML Can Thwart Phishing Attacks. Forbes [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2020/08/12/5-ways-machine-learning-can-thwart-phishing-attacks/?sh=6b8698871035 [Accessed September 7, 2023].
[19] Corona I., Biggio B., and Contini M. (2017): DeltaPhish: Detecting phishing webpages in compromised websites. In: Foley S, Gollmann D, Snekkenes E, eds, *Computer Security —ESORIC. Lecture Notes in Computer Science.* Vol.10492. Springer; p.370-388, 2017.
[20] Fujita M., *et al*. (2015): An Attempt to Memorize Strong Passwords while Playing Games. In 2015 18th International Conference on Network-Based Information Systems (NBiS). 2015, pp. 264-268.
[21] Gomes, L., Deshmukh, A., & Anute, N. (2022, July 14): Cyber Security and Internet Banking: Issues and Preventive Measures. *Journal of Information Technology and Sciences*, 8(2), 31–42. https://doi.org/10.46610/joits.2022.v08i02.005
[22] Gupta B.B., Arachchilage N.A., and Psannis K.E. (2018): Defending against phishing attacks: taxonomy of methods, current issues and future directions, *Telecommun.* Syst. 67 (2), pp. 247267.
[23] He, D., Chan, S., & Guizani, M. (2015, February). Mobile application security: malware threats and defenses. *IEEE Wireless Communications*, 22(1), 138–144. https://doi.org/10.1109/mwc.2015.7054729
[24] Hota H.S., Shrivas A.K., Hota R., (2018): An Ensemble Model for Detecting Phishing Attack with Proposed Remove-Replace Feature Selection Technique, *Procedia Computer Science*, Vol. 132, p.900-907, 2018. https://doi.org/10.1016/j.procs.2018.05.103. Available: https://www.sciencedirect.com/science/article/pii/S1877050918308354
[25] Jamil H., Hussain F., and Khan S. A. (2021): Phishing Attacks: A Review, *IEEE Communications Surveys & Tutorials,* Vol.23, No. 4, pp.2835-2869.
[26] Jansen J. (2015), Studying Safe Online Banking Behavior: A Protection Motivation Theory Approach. *In HAISA*, pp. 120-130. 2015.
[27] Joshi K., et al. (2023): Machine-Learning Techniques for Predicting Phishing Attacks in Blockchain Networks: A Comparative Study, *Algorithms*, Vol. 16, No. 366. 2023. Available: https://doi.org/10.3390/a16080366 [Accessed September 7, 2023]
[28] Kagantech (2023): Exposing the Underbelly of Fake Transfer Fraud!!. Instagram [Online]. Available: https://www.instagram.com/p/Cv6f5C_IdDe/ [Accessed September 7, 2023].
[29] Kanhere S., *et al.* (2018): Phishing: A Comprehensive Study, *IEEE Communications Surveys & Tutorials,* Vol.20, No.4, p.2756-2789.
[30] Khedmatgozar, H. R., & Shahnazi, A. (2017, March 8): The role of dimensions of perceived risk in adoption of corporate internet banking by customers in Iran. *Electronic Commerce Research*, 18(2), 389–412. https://doi.org/10.1007/s10660-017-9253-z
[31] KPMG (2014): Banking industry customer satisfaction survey. KPMG Professional Services, Lagos, available at: www.Kpmg.com.
[32] Lokesh G. H. and BoreGowda, G. (2020) Phishing website detection based on effective machine learning approach, *J. Cyber Sec. Technol*. 114.
[33] Mahmoud O. and Hesham H. (2022): An Empirical Study Towards an Automatic Phishing Attack Detection Using Ensemble Stacking Model. *Future Computing and Informatics Journal*: Vol. 7: Iss.1, Article 1. DOI: http://Doi.org/10.54623/fue.fcij.7.1.1 Available at: https://digitalcommons.aaru.edu.jo/fcij/vol7/iss1/1 [Accessed September 7, 2023]
[34] Michael, C. (2022): Fake bank alerts put small businesses at risk. BusinessDay [Online]. Available: https://businessday.ng/technology/article/fake-bank-alerts-put-small-businesses-at-risk/ [Accessed September 7, 2023].
[35] Mitchell T. (1997): Machine Learning. McGraw-Hill International Edition.
[36] Mitrobe (2022): Top 5 Apps in Nigeria That Does Fake Bank Alerts. NGSUP NETWORK [Online]. Available: https://ngsup.com/top-5-apps-in-nigeria-that-does-fake-bank-alerts/#ixzz7ZHcohx4O [Accessed September 7, 2023].
[37] Mitrobe Network (2022): Scam Alert| 5 Apps That Can Be Used to Do Fake Bank Alerts. YouTube [Online]. Available: https://www.youtube.com/watch?v=poR9GbKhIG0 [Accessed September 7, 2023].
[38] Mridha F. M., Nur K., Saha K. A., & Adnan A. (2017, February 15). A New Approach to Enhance Internet Banking Security. *International Journal of Computer Applications*, 160(8), 35–39. https://doi.org/10.5120/ijca2017913093
[39] Naqvi, B., et al (2023), "Mitigation strategies against the phishing attacks: A systematic literature review", *Computers & Security*, Vol.132. Elsevier Ltd. Available: https://doi.org/10.1016/j.cose.2023.103387. [Accessed September 7, 2023]
[40] Orunsolu A.A., Sodiya A.S., and Akinwale A.T. (2022): A predictive model for phishing detection, *Journal of King Saud University – Computer and Information Sciences*, Vol. 34, p. 232–247. Available: https://doi.org/10.1016/j.jksuci.2019.12.005 [Accessed September 7, 2023]
[41] Othman M. and Hassan H. (2022): An Empirical Study Towards an Automatic Phishing Attack Detection Using Ensemble Stacking Model. *Future Computing and Informatics Journal*, Vol. 7, Iss 1.
[42] Parekh S., *et al.* (2018): A new method for detection of phishing websites: Url detection. *In 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT),* p.949–952, 2018. IEEE.
[43] Rahman S.S.M.M, et al. (2020): Performance assessment of multiple machine learning classifiers for detecting the phishing URLs, in: *Data Engineering and Communication Technology*, Springer, pp. 285–296.
[44] Rao R. and Pais A. (2019): Detection of phishing websites using an efficient feature-based machine learning framework, *Neural Comput Appl*., Vol. 31, No. 8, p.3851–3873.
[45] Shaikh A., Shabut A., and Hossain A. (2016), A literature review on phishing crime, prevention review and investigation of gaps, p.9-15. Available: https://ieeexplore.ieee.org/document/7916190 [Accessed September 7, 2023].
[46] Shie E. W. S. (2020): Critical analysis of current research aimed at improving detection of phishing attacks, Selected computing research papers, p. 45. 2020.

[47] Stallings W. (2020): Data and computer communications, (11th ed.). Pearson.
[48] Urias, V.E., et al. (2017), Technologies to enable cyber deception, in: 2017 International Carnahan Conference on Security Technology (ICCST), *IEEE*, pp. 16.
[49] Valente, A., et al. (2022): Analysis of Academic Databases for Literature Review in the Computer Science Education Field. In: 2022 IEEE Frontiers in Education Conference (FIE), IEEE, pp. 1–7.
[50] Volkamer M., et al., (2017): User experiences of TORPEDO: TOoltip-poweRed Phishing Email DetectiOn", *Computers & Security*, Vol.71, p.100-113, 2017. ISSN 0167-4048, Available: https://doi.org/10.1016/j.cose.2017.02.004. [Accessed September 7, 2023].
[51] Vrbanˇciˇc G., Fister Jr I., & Podgorelec V. (2018): Swarm intelligence approaches for parameter setting of deep learning neural network: Case study on phishing websites classification, In Proceedings of the 8th international conference on web intelligence, mining and semantics, p.1–8,.
[52] Yang P., Zhao G., and Zeng P. (2019): Phishing website detection based on multidimensional features driven by deep learning. *IEEE Access 7*, p.15196–15209.
[53] Zhang X. and Wang J. (2023): A comparative study of feature selection techniques for finite-state transducers, *Information Sciences*, vol. 575, p.123-136.
[54] Zheng W. and Jin M. (2018) A Comparative Study Of Feature Selection methods", International Journal on Natural Language Computing (IJNLC), Vol.7, No.5. Available: https://www.researchgate.net/publication/328904014_A_Comparative_Study_of_Feature_Selection_Methods [Accessed Sep 15 2023].
[55] Zhu E., et al (2020): DTOF-ANN: an artificial neural network phishing detection model based on decision tree and optimal features. *Appl. Soft Comput*., 106505.

Authors Profile

Dr. Seun Ebiesuwa holds a first degree in Computer Engineering from the Lagos State University. Dr. Ebiesuwa bagged a Master's and a Ph.D degree in Computer Science from Babcock University. He is a lecturer in the Department of Computer Science, Babcock University and he specializes in Information Systems. Dr. Seun Ebiesuwa has over forty-five academic publications in internationally peer-reviewed journals of Computer Science in the areas of Artificial Intelligence, Data Analytics, Machine Learning and Medical Informatics. He has made several academic presentations in Workshops, Seminars, Symposiums and Conferences.

Dipo Tepede is a recognized expert in Process and Project Management, holding a Master Black Belt in Lean Six Sigma, along with certifications as a Professional Project Manager and Business Analyst from the Project Management Institute, and as a SAFe Scrum Master from Scaled Agile. He obtained his undergraduate degree from Obafemi Awolowo University and an MBA from the University of Gavle, Sweden. His academic journey expanded to Arden University in the United Kingdom, where he explored a Master of Science in Data Analysis. Currently pursuing a Ph.D. in Cybersecurity at Babcock University, his research focuses on Machine Learning, Data Analytics, and Artificial Intelligence, showcasing his commitment to advancing knowledge in the field.