Awareness," *Comput. Secur.*, vol. 88, p. 101640, 2020, doi: 10.1016/j.cose.2019.101640.
[5] H. Aldawood and G. Skinner, "Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review," *Proc. 2018 IEEE Int. Conf. Teaching, Assessment, Learn. Eng. TALE 2018*, no. December, pp. 62–68, 2019, doi: 10.1109/TALE.2018.8615162.
[6] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Futur. Internet*, vol. 11, no. 4, 2019, doi: 10.3390/FI11040089.
[7] N. N. Pokrovskaia and S. O. Snisarenko, "Social engineering and digital technologies for the security of the social capital' development," *Proc. 2017 Int. Conf. "Quality Manag. Transp. Inf. Secur. Inf. Technol. IT QM IS 2017*, pp. 16–18, 2017, doi: 10.1109/ITMQIS.2017.8085750.
[8] A. M. Aroyo, F. Rea, G. Sandini, and A. Sciutti, "Trust and Social Engineering in Human Robot Interaction: Will a Robot Make You Disclose Sensitive Information, Conform to Its Recommendations or Gamble?," *IEEE Robot. Autom. Lett.*, vol. 3, no. 4, pp. 3701–3708, 2018, doi: 10.1109/LRA.2018.2856272.
[9] M. Chargo, "You've Been Hacked: How to Better Incentivize Corporations to Protect Consumers' Data Michael," *Tennessee J. Bus. Law*, vol. 20, pp. 6–23, 2004.
[10] J. Tan, W. X. Tee, A. Parsons, and A. Radlett, "Asean cyberthreat assessment 2021," *Interpol*, p. 5, 2021, [Online]. Available: https://www.interpol.int/content/download/16106/file/ASEAN Cyberthreat Assessment 2021 - final.pdf.
[11] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," *J. Comput. Inf. Syst.*, vol. 62, no. 1, pp. 82–97, Jan. 2022, doi: 10.1080/08874417.2020.1712269.
[12] G. Costantino, A. La Marra, F. Martinelli, and I. Matteucci, "CANDY: A social engineering attack to leak information from infotainment system," *IEEE Veh. Technol. Conf.*, vol. 2018-June, pp. 1–5, 2018, doi: 10.1109/VTCSpring.2018.8417879.
[13] A. Birajdar and T. N. N., "APPEARS Framework for evaluating Gamified Cyber Security Awareness Training," in *2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS)*, 2022, pp. 1–8, doi: 10.1109/IC3SIS54991.2022.9885399.
[14] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *J. Big Data*, vol. 7, no. 1, 2020, doi: 10.1186/s40537-020-00318-5.
[15] A. Ključnikov, L. Mura, and D. Sklenár, "Information security management in smes: Factors of success," *Entrep. Sustain. Issues*, vol. 6, no. 4, pp. 2081–2094, 2019, doi: 10.9770/jesi.2019.6.4(37).
[16] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," *Comput. Secur.*, vol. 106, p. 102267, 2021, doi: 10.1016/j.cose.2021.102267.
[17] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, "Information security governance challenges and critical success factors: Systematic review," *Comput. Secur.*, vol. 99, p. 102030, 2020, doi: 10.1016/j.cose.2020.102030.
[18] B. Ghimire and D. B. Rawat, "Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8229–8249, 2022, doi: 10.1109/JIOT.2022.3150363.
[19] A. Corallo, M. Lazoi, and M. Lezzi, "Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts," *Comput. Ind.*, vol. 114, p. 103165, 2020, doi: 10.1016/j.compind.2019.103165.
[20] A. K. Jain and B. B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," *Enterp. Inf. Syst.*, vol. 16, no. 4, pp. 527–565, Apr. 2022, doi: 10.1080/17517575.2021.1896786.
[21] Y. A. Alsariera, V. E. Adeyemo, A. O. Balogun, and A. K. Alazzawi, "AI Meta-Learners and Extra-Trees Algorithm for the Detection of Phishing Websites," *IEEE Access*, vol. 8, pp. 142532–142542, 2020, doi: 10.1109/ACCESS.2020.3013699.
[22] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," *Front. Comput. Sci.*, vol. 3, no. March, pp. 1–23, 2021, doi: 10.3389/fcomp.2021.563060.
[23] R. Alabdan, "Phishing attacks survey: Types, vectors, and technical approaches," *Futur. Internet*, vol. 12, no. 10, pp. 1–39, 2020, doi: 10.3390/fi12100168.
[24] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommun. Syst.*, vol. 76, no. 1, pp. 139–154, 2021, doi: 10.1007/s11235-020-00733-2.
[25] R. Wash, "How Experts Detect Phishing Scam Emails," *Proc. ACM Human-Computer Interact.*, vol. 4, no. CSCW2, 2020, doi: 10.1145/3415231.
[26] J. Wu *et al.*, "Who Are the Phishers? Phishing Scam Detection on Ethereum via Network Embedding," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 52, no. 2, pp. 1156–1166, 2022, doi: 10.1109/TSMC.2020.3016821.
[27] G. Egozi, "Phishing Email Detection Using Robust NLP Techniques," *2018 IEEE Int. Conf. Data Min. Work.*, pp. 7–12, 2018, doi: 10.1109/ICDMW.2018.00009.
[28] P. Xia *et al.*, "Trade or Trick? Detecting and Characterizing Scam Tokens on Uniswap Decentralized Exchange," *Proc. ACM Meas. Anal. Comput. Syst.*, vol. 5, no. 3, 2021, doi: 10.1145/3491051.
[29] M. A. Mendoza, "Cibersegurança ou segurança da informação? Explicando a diferença," 2017. https://www.welivesecurity.com/br/2017/01/17/ciberseguranca-ou-seguranca-da-informacao/.
[30] H. Ahmadian and A. Sabri, "Teknik Penyerangan Phishing Pada Social," vol. 2, no. 1, 2021.
[31] C. M. R. da Silva, E. L. Feitosa, and V. C. Garcia, "Heuristic-based strategy for Phishing prediction: A survey of URL-based approach," *Comput. Secur.*, vol. 88, p. 101613, 2020, doi: 10.1016/j.cose.2019.101613.
[32] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios," *Comput. Secur.*, vol. 59, pp. 186–209, 2016, doi: 10.1016/j.cose.2016.03.004.
[33] H. Abroshan, J. Devos, G. Poels, and E. Laermans, "Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process," *IEEE Access*, vol. 9, pp. 44928–44949, 2021, doi: 10.1109/ACCESS.2021.3066383.
[34] P. L. Gallegos-Segovia, P. E. Vintimilla-Tapia, J. F. Bravo-Torres, I. F. Yuquilima-Albarado, V. M. Larios-Rosillo, and J. D. Jara-Saltos, "Social engineering as an attack vector for ransomware," *2017 Chil. Conf. Electr. Electron. Eng. Inf. Commun. Technol. CHILECON 2017 - Proc.*, vol. 2017-Janua, pp. 1–6, 2017, doi: 10.1109/CHILECON.2017.8229528.
[35] Zuhair, Hiba & Selamat, Ali & Salleh, Mazleena. (2016). Feature selection for phishing detection: A review of research. International Journal of Intelligent Systems Technologies and Applications. 15. 147. 10.1504/IJISTA.2016.076495.
[36] G. Varshney, M. Misra, and P. K. Atrey, "A survey and classi fi cation of web phishing detection schemes," 2016, doi: 10.1002/sec.
[37] S. Salloum, T. Gaber, S. Vadera, and K. Shaalan, "Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey," *Procedia Comput. Sci.*, vol. 189, pp. 19–28, 2021, doi: https://doi.org/10.1016/j.procs.2021.05.077.
[38] T. Lin *et al.*, "Susceptibility to Spear-Phishing Emails," *ACM Trans. Comput. Interact.*, vol. 26, no. 5, pp. 1–28, 2019, doi: 10.1145/3336141.
[39] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions," *SN Comput. Sci.*, vol. 2, no. 3, pp. 1–18, 2021, doi: 10.1007/s42979-021-00557-0.
[40] A. K. Jain and B. B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," *Enterp. Inf. Syst.*, vol. 00, no. 00, pp. 1–39, 2021, doi: 10.1080/17517575.2021.1896786.
[41] X. Chen, X. Liu, L. Zhang, and C. Tang, "Optimal Defense Strategy Selection for Spear-Phishing Attack Based on a Multistage Signaling Game," *IEEE Access*, vol. 7, pp. 19907–19921, 2019, doi: 10.1109/ACCESS.2019.2897724.
[42] I. Vayansky and S. Kumar, "Phishing – challenges and solutions," *Comput. Fraud Secur.*, vol. 2018, no. 1, pp. 15–20, 2018, doi: 10.1016/S1361-3723(18)30007-1.
[43] N. Farhana, M. Zaharon, and M. M. Ali, "Factors Affecting Awareness of Phishing Among Generation Y," *Asia-Pacific Manag. Account. J.*, no. April 2021, 2021, [Online]. Available: https://ir.uitm.edu.my/id/eprint/2861/.
[44] S. S. Lin, S. L. Shen, A. Zhou, and Y. S. Xu, "Risk Assessment and Management of Excavation System Based On Fuzzy Set Theory and Machine Learning Methods," *Autom. Constr.*, vol. 122, no. November 2020, p. 103490, 2021, doi: 10.1016/j.autcon.2020.103490.