**REFERENCES**

[1] A. Aleroud and L. Zhou, "Phishing environments,

techniques, and countermeasures: A survey," Computers &

Security, vol. 68, pp. 160-196, 2017.

[2] I. Vayansky and S. Kumar, "Phishing–challenges and

solutions," Computer Fraud & Security, vol. 2018, pp. 15-20,

2018.

[3] E. J. Williams, et al., "Exploring susceptibility to phishing

in the workplace," International Journal of Human-Computer

Studies, vol. 120, pp. 1-13, 2018.

[4] A. Odeh, et al., "Machine LearningTechniquesfor

Detection of Website Phishing: A Review for Promises and

Challenges," in 2021 IEEE 11th Annual Computing and

Communication Workshop and Conference (CCWC), 2021,

pp. 0813-0818.

[5] A. Odeh, et al., "Efficient Detection of Phishing Websites

Using Multilayer Perceptron," 2020.

[6] A. Odeh, et al., "PHIBOOST-a novel phishing detection

model using Adaptive boosting approach," Jordanian Journal

of Computers and Information Technology (JJCIT), vol. 7,

2021.

[7] K. L. Chiew, et al., "A survey of phishing attacks: Their

types, vectors and technical approaches," Expert Systems with

Applications, vol. 106, pp. 1-20, 2018.

[8] M. Al-Fayoumi, et al., "Intelligent association

classification technique for phishing website detection,"

International Arab Journal of Information Technology, vol.

17, pp. 488-496, 2020.

[9] Y. Kwak, et al., "Why do users not report spear phishing

emails?," Telematics and Informatics, vol. 48, p. 101343,

2020.

[10] A. Odeh, et al., "PHISHING WEBSITE

DETECTION USING MULTILAYER PERCEPTRON."

[11] G. Sonowal and K. Kuppusamy, "PhiDMA–A

phishing detection model with multi-filter approach," Journal

of King Saud University-Computer and Information Sciences,

vol. 32, pp. 99-112, 2020.

[12] A. ODEH, et al., "Efficient Prediction Of Phishing

Websites Using Multilayer Perceptron (Mlp)," Journal of

Theoretical and Applied Information Technology, vol. 98,

2020. [13] I. Keshta and A. Odeh, "Security and privacy of

electronic health records: Concerns and challenges," Egyptian

Informatics Journal, vol. 22, pp. 177-183, 2021.

[14] R. Faek, et al., "Exposing Bot Attacks Using

Machine Learning and Flow Level Analysis," in International

Conference on Data Science, E-learning and Information

Systems 2021, 2021, pp. 99-106.

[15] O. K. Sahingoz, et al., "Machine learning based

phishing detection from URLs," Expert Systems with

Applications, vol. 117, pp. 345-357, 2019.

[16] A. Oest, et al., "Inside a phisher's mind:

Understanding the anti-phishing ecosystem through phishing

kit analysis," in 2018 APWG Symposium on Electronic Crime

Research (eCrime), 2018, pp. 1-12.

[17] A. Abbasi, et al., "The phishing funnel model: A

design artifact to predict user susceptibility to phishing

websites," Information Systems Research, vol. 32, pp. 410-

436, 2021.

[18] P. Yang, et al., "Phishing website detection based on

multidimensional features driven by deep learning," IEEE

Access, vol. 7, pp. 15196-15209, 2019.

[19] D. A. Pisner and D. M. Schnyer, "Support vector

machine," in Machine Learning, ed: Elsevier, 2020, pp. 101-

121.

[20] D. Berrar, "Bayes’ theorem and naive Bayes

classifier," Encyclopedia of Bioinformatics and

Computational Biology: ABC of Bioinformatics; Elsevier

Science Publisher: Amsterdam, The Netherlands, pp. 403-

412, 2018.

[21] S. Athey, et al., "Generalized random forests," The

Annals of Statistics, vol. 47, pp. 1148-1178, 2019.

0011