[1] Sahar Abdelnabi, Katharina Krombholz, and Mario Fritz. 2020. VisualPhishNet: Zero-day phishing website detection by visual similarity.

In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (Virtual Event, USA) (CCS’20). ACM, New

York, 1681–1698.

[2] Giovanni Apruzzese, Michele Colajanni, Luca Ferretti, and Mirco Marchetti. 2019. Addressing adversarial attacks against security sys-

tems based on machine learning. In Proceedings of the 2019 11th International Conference on Cyber Conflict (CyCon’19), Vol. 900. ieeex-

plore.ieee.org, 1–18.

[3] Giovanni Apruzzese, Mauro Conti, and Ying Yuan. 2022. SpacePhish: The evasion-space of adversarial attacks against phishing website

detectors using machine learning. arXiv preprint arXiv:2210.13660 (2022).

[4] Giovanni Apruzzese, Pavel Laskov, Edgardo Montes de Oca, Wissam Mallouli, Luis Búrdalo Rapa, Athanasios Vasileios Grammatopou-

los, and Fabio Di Franco. 2022. The role of machine learning in cybersecurity. Digital Threats: Research and Practice (Jul 2022).

https://doi.org/10.1145/3545574 Just Accepted.

[5] Battista Biggio, Igino Corona, Davide Maiorca, Blaine Nelson, Nedim Šrndić, Pavel Laskov, Giorgio Giacinto, and Fabio Roli. 2013. Eva-

sion attacks against machine learning at test time. In Proceedings of the Joint European Conference on Machine Learning and Knowledge

Discovery in Databases. Springer, 387–402.

[6] CUJOAI. 2021. Announcing the Winners of the 2021 MLSEC. https://cujo.com/announcing-the-winners-of-the-2021-machine-

learning-security-evasion-competition/.

[8] Bin Liang, Miaoqiang Su, Wei You, Wenchang Shi, and Gang Yang. 2016. Cracking classifiers for evasion: A case study on the Google’s

phishing pages filter. In Proceedings of the 25th International Conference on World Wide Web (WWW’16) (Montréal, Québec, Canada).

International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 345–356.

[9] Peng Peng, Limin Yang, Linhai Song, and Gang Wang. 2019. Opening the blackbox of VirusTotal: Analyzing online phishing scan engines.

In Proceedings of the Internet Measurement Conference (IMC’19) (Amsterdam, Netherlands). ACM, New York, NY, USA, 478–485.

[13] Fu Song, Yusi Lei, Sen Chen, Lingling Fan, and Yang Liu. 2021. Advanced evasion attacks and mitigations on practical ML-based phishing

website classifiers. International Journal of Intelligent Systems 36, 9 (2021), 5210–5240.

[16] Guang Xiang, Jason Hong, Carolyn P. Rose, and Lorrie Cranor. 2011. CANTINA+: A feature-rich machine learning framework for

detecting phishing web sites. ACM Trans. Inf. Syst. Secur. 14, 2 (Sept. 2011), 1–28.

[17] Penghui Zhang, Adam Oest, Haehyun Cho, Zhibo Sun, R. C. Johnson, Brad Wardman, Shaown Sarker, Alexandros Kapravelos, Tiffany

Bao, Ruoyu Wang, Yan Shoshitaishvili, Adam Doupé, and Gail-Joon Ahn. 2021. CrawlPhish: Large-scale analysis of client-side cloaking

techniques in phishing. In Proceedings of the2021 IEEE Symposium on Security and Privacy (SP’21). ieeexplore.ieee.org, 1109–1124.