

Bibliography

- [1] Saracco, Roberto. “A never ending decrease of technology cost”. In: *IEEE Future Directions* (Oct. 2017). URL: <https://cmte.ieee.org/futuredirections/2017/10/18/a-never-ending-decrease-of-technology-cost/>.
- [2] Radicati, Sara. “Email statistics report, 2015-2019”. In: *The Radicati Group, INC., A Technology Market Research Firm, Palo Alto, CA, USA April* (2015).
- [3] Cvetičanin, Nikolina. *What’s On the Other Side of Your Inbox – 20 SPAM Statistics for 2021*. 2021. URL: <https://dataprot.net/statistics/spam-statistics>. (visited on 04/23/2021).
- [4] Mallikarjunappa, Basavaraju and Prabhakar, Dr. “A Novel Method of Spam Mail Detection using Text Based Clustering Approach”. In: *International Journal of Computer Applications* 5 (Aug. 2010), p. 15. DOI: 10.5120/906-1283.
- [5] Chawla, Minal and Chouhan, Siddharth. “A Survey of Phishing Attack Techniques”. In: *International Journal of Computer Applications* 93 (May 2014), pp. 32–35. DOI: 10.5120/16197-5460.
- [6] Chen, Rui, Gaia, Joana, and Rao, H. Raghav. “An examination of the effect of recent phishing encounters on phishing susceptibility”. In: *Decision Support Systems* 133 (2020), p. 113287. ISSN: 0167-9236. DOI: <https://doi.org/10.1016/j.dss.2020.113287>. URL: <https://www.sciencedirect.com/science/article/pii/S0167923620300427>.
- [7] Karla Pak, Doug Shade. *Consumer Fraud Victims - AARP Foundation Study*. 2011. URL: <https://www.aarp.org/money/scams-fraud/info-03-2011/fraud-victims-11.html>. (visited on 04/25/2021).

- [8] Harrison, Brynne et al. "Examining the Impact of Presence on Individual Phishing Victimization". In: *2015 48th Hawaii International Conference on System Sciences*. 2015, pp. 3483–3489. DOI: 10.1109/HICSS.2015.419.
- [9] Ferrara, Emilio. "The History of Digital Spam". In: *Commun. ACM* 62.8 (July 2019), pp. 82–91. ISSN: 0001-0782. DOI: 10.1145/3299768. URL: <https://doi.org/10.1145/3299768>.
- [10] Ghazi-Tehrani, Adam Kavon and N.Pontell, Henry. "Phishing Evolves: Analyzing the Enduring Cybercrime". In: *Victims & Offenders* 16.3 (2021), pp. 316–342. DOI: 10.1080/15564886.2020.1829224. eprint: <https://doi.org/10.1080/15564886.2020.1829224>. URL: <https://doi.org/10.1080/15564886.2020.1829224>.
- [11] Egan, Gretel. "2020 'State of the Phish': Security Awareness Training, Email Reporting More Critical as Targeted Attacks Spike". In: *State of The Fish* (Jan. 2020). URL: <https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical>.
- [12] Abroshan, Hossein et al. "Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process". In: *IEEE Access* 9 (2021), pp. 44928–44949. DOI: 10.1109/ACCESS.2021.3066383. URL: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9380285>.
- [13] Ferreira, Ana and Lenzi, Gabriele. "An analysis of social engineering principles in effective phishing". In: *2015 Workshop on Socio-Technical Aspects in Security and Trust*. 2015, pp. 9–16. DOI: 10.1109/STAST.2015.10.
- [14] Ludl, Christian et al. "On the effectiveness of techniques to detect phishing sites". In: *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer Berlin Heidelberg, 2007, pp. 20–39. ISBN: 978-3-540-73614-1.
- [15] Alghamdi, H. "Can Phishing Education Enable Users To Recognize Phishing Attacks?" In: *Masters dissertation, Technological University Dublin* (2017). DOI: 10.21427/D7DK8T. URL: <https://arrow.tudublin.ie/scschcomdis/99/>.
- [16] Polit, Denise F and Beck, Cheryl Tatano. *Nursing research: Principles and methods*. Lippincott Williams & Wilkins, 2004, pp. 19, 350–251.