APENDIX to: Defending Against Phishing Attacks on Cloud-Systems: What Has Been Studied?

Carlos Eduardo Araújo Cardoso Cidrão, Oskar Hermansson and Simon Hacks[a]

Department of Computer and Systems Sciences, Stockholm University, Stockholm, Sweden

carloz.eduardo99@gmail.com, oskar.c.hermansson@gmail.com, simon.hacks@dsv.su.se

Keywords: Phishing, Cloud, Cyber Defense, Systematic Literature Review.

Abstract: Phishing attacks, a cybercrime where attackers deceive victims into revealing personal and financial information, present significant threats to cloud-based systems. Securing these environments has become paramount with the growing adoption of cloud services. This study addresses the research question: "What is the overall perception of strategies in scientific publications to counter phishing attacks targeting cloud services?" Using a systematic literature review approach, the research synthesized findings from 13 selected scientific articles, focusing on technical and social defense strategies against phishing.

The key findings indicate that the human factor remains a critical vulnerability. At the same time, robust technical solutions such as advanced authentication methods, Intrusion Detection Systems (IDS), and machine learning algorithms exist. Effective phishing prevention requires a combination of technical defenses and comprehensive user education programs to enhance awareness and response to phishing attempts. The study also highlights the need to continuously adapt defense mechanisms to counter the evolving sophistication of phishing strategies. Despite the progress in technical defenses, the study suggests a greater integration of social aspects into technical solutions to mitigate the risks effectively. Future research should focus on developing targeted defense strategies for specific cloud service models and exploring the intersection of artificial intelligence and phishing to enhance security further.

[a] https://orcid.org/0000-0003-0478-9347

Table 1: Coding Results

Theme	Category	Code	Article
Defense Methods	Technical Methods	Software Security	(Chandra et al., 2015; Chaudhry et al., 2016; Goel et al., 2017; Vayansky and Kumar, 2018; Prasad et al., 2022)
		Communication Security	(Chaudhry et al., 2016; Wu et al., 2017)
		Network Security	(Chandra et al., 2015; Chaudhry et al., 2016; Vayansky and Kumar, 2018; Prasad et al., 2022; Althamary and El-Alfy, 2017; Gutierrez et al., 2018; Pham et al., 2018; Preethi et al., 2023)
		System and Data Protection	(Chandra et al., 2015; Chaudhry et al., 2016; Goel et al., 2017; Prasad et al., 2022; Wu et al., 2017; Althamary and El-Alfy, 2017)
		Cloud Security	(Chandra et al., 2015; Vayansky and Kumar, 2018; Wu et al., 2017; Gutierrez et al., 2018; Pham et al., 2018; Preethi et al., 2023; Allodi et al., 2019; Karthika et al., 2023; Jha et al., 2022)
	Social Methods	Communication	(Chaudhry et al., 2016; Pham et al., 2018)
		Education	(Chandra et al., 2015; Chaudhry et al., 2016; Goel et al., 2017; Vayansky and Kumar, 2018; Althamary and El-Alfy, 2017; Allodi et al., 2019)
		Awareness	(Chandra et al., 2015; Goel et al., 2017; Althamary and El-Alfy, 2017; Allodi et al., 2019)
	Algorithmical Methods	Machine Learning	(Chandra et al., 2015; Chaudhry et al., 2016; Vayansky and Kumar, 2018; Prasad et al., 2022; Wu et al., 2017; Gutierrez et al., 2018; Pham et al., 2018; Preethi et al., 2023; Karthika et al., 2023; Jha et al., 2022)
		Automated Analysis	(Chaudhry et al., 2016; Prasad et al., 2022; Karthika et al., 2023)
		Email Security	(Chaudhry et al., 2016)
		Cryptography	(Chandra et al., 2015; Karthika et al., 2023)

Table 1: Coding Results

Theme	Category	Code	Article
Evaluation	Criteria	Performance	(Chaudhry et al., 2016; Vayansky and Kumar, 2018; Prasad et al., 2022; Wu et al., 2017; Althamary and El-Alfy, 2017; Gutierrez et al., 2018; Preethi et al., 2023; Pham et al., 2018; Karthika et al., 2023; Jha et al., 2022)
		Efficiency	(Chandra et al., 2015; Wu et al., 2017; Gutierrez et al., 2018; Preethi et al., 2023)
		Reliability	(Chaudhry et al., 2016; Preethi et al., 2023; Karthika et al., 2023)
		User Behavior	(Chaudhry et al., 2016; Goel et al., 2017; Vayansky and Kumar, 2018; Althamary and El-Alfy, 2017)
Challenges	Technical Challenges	Machine Learning Challenges	(Prasad et al., 2022; Gutierrez et al., 2018; Preethi et al., 2023; Karthika et al., 2023; Jha et al., 2022)
		Cloud Security	(Chandra et al., 2015; Prasad et al., 2022; Wu et al., 2017; Althamary and El-Alfy, 2017; Gutierrez et al., 2018; Pham et al., 2018; Preethi et al., 2023; Jha et al., 2022)
		Blockchain	(Karthika et al., 2023)
		Traditional Methods	(Chandra et al., 2015; Wu et al., 2017; Althamary and El-Alfy, 2017; Gutierrez et al., 2018; Pham et al., 2018; Preethi et al., 2023; Jha et al., 2022)
	Social Challenges	User-Related Challenges	(Goel et al., 2017; Prasad et al., 2022; Karthika et al., 2023)
		Education and Training	(Goel et al., 2017)
		Cognitive Limitations	(Goel et al., 2017)
		Psychological Factors	(Goel et al., 2017; Vayansky and Kumar, 2018)
		Individual and Cultural Differences	(Goel et al., 2017)

REFERENCES

Allodi, L., Chotza, T., Panina, E., and Zannone, N. (2019). The need for new antiphishing measures against spear-phishing attacks. *IEEE Security & Privacy*, 18(2):23–34.

Althamary, I. A. and El-Alfy, E.-S. M. (2017). A more secure scheme for captcha-based authentication in cloud environment. In *2017 8th International Conference on Information Technology (ICIT)*, pages 405–411. IEEE.

Chandra, J. V., Challa, N., and Pasupuleti, S. K. (2015). Intelligence based defense system to protect from advanced persistent threat by means of social engineering on social cloud platform. *Indian Journal of Science and Technology*.

Chaudhry, J. A., Chaudhry, S. A., and Rittenhouse, R. G. (2016). Phishing attacks and defenses. *International journal of security and its applications*, 10(1):247–256.

Goel, S., Williams, K., and Dincelli, E. (2017). Got phished? internet security and human vulnerability. *Journal of the Association for Information Systems*, 18(1):2.

Gutierrez, C. N., Kim, T., Della Corte, R., Avery, J., Goldwasser, D., Cinque, M., and Bagchi, S. (2018). Learning from the ones that got away: Detecting new forms of phishing attacks. *IEEE Transactions on Dependable and Secure Computing*, 15(6):988–1001.

Jha, B., Atre, M., and Rao, A. (2022). Detecting cloud-based phishing attacks by combining deep learning models. In *2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*, pages 130–139. IEEE.

Karthika, R., Valliyammai, C., and Naveena, M. (2023). Phish block: A blockchain framework for phish detection in cloud. *Computer Systems Science & Engineering*, 44(1).

Pham, C., Nguyen, L. A., Tran, N. H., Huh, E.-N., and Hong, C. S. (2018). Phishing-aware: A neuro-fuzzy approach for anti-phishing on fog networks. *IEEE Transactions on Network and Service Management*, 15(3):1076–1089.

Prasad, V. K., Dansana, D., Mishra, B. K., and Bhavsar, M. (2022). Intensify cloud security and privacy against phishing attacks. *ECS Transactions*, 107(1):1387.

Preethi, P., Ramadevi, P., Akshaya, K., Sangamitra, S., and Pritikha, A. (2023). Analysis of phishing attack in distributed cloud systems using machine learning. In *2023 Second International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT)*, pages 1–5. IEEE.

Vayansky, I. and Kumar, S. (2018). Phishing–challenges and solutions. *Computer Fraud & Security*, 2018(1):15–20.

Wu, W., Hu, S., Yang, X., Liu, J. K., and Au, M. H. (2017). Towards secure and cost-effective fuzzy access control in mobile cloud computing. *Soft Computing*, 21:2643–2649.