Vol.1 No.1 October 2024: 7-11
International Journal of Computer Science and Humanitarian AI (IJCSHAI)

e-ISSN: 3064-4372
DOI: 10.21512/ijcshaijournal.v1i1.12155

A Systematic Literature Review: Cyber Attack: Phishing Environments, Techniques, and Detection Mechanism

Cindy Natasya[1], Irvin[2], Alexander Agung Santoso Gunawan[3*]

[1-2]Mathematics Department, School of Computer Science,
[3]Computer Science Department, School of Computer Science,
Bina Nusantara University,
Jakarta, Indonesia 11480

cindy.natasya@binus.ac.id; irvin002@binus.ac.id; aagung@binus.edu;

***Abstract*— In this digital era, phishing has attacked many platforms such as email, website, message, link form. Phishing is an act of creating a website that is exactly like the original website that is used to take someone's personal data. Phishing causes loss of customer confidence to use any application or website. Most of the victims of phishing are people who do not understand phishing or an organization. This kind of cyber-attacks consist of various types and countermeasures that need to be considered for the public user to prevent phishing based on phishing techniques, educate individuals about these attacks, and encourage the use of phishing prevention techniques. This paper consists of types of phishing and awareness to wary of phishing to overcome them. Therefore, the goal of this study is to identify the most typical environments for phishing attacks in order to ascertain the most popular media and technique. The authors of this study plan to conduct a Systematic Literature Review (SLR) of studies that have been done on the subject that was just described. The authors come to the overall conclusion that a website is the ideal option for phishing attacks using social engineering techniques. Additionally, the authors offer numerous suggestions for preventing phishing with various techniques. However, the most effective defense against phishing attacks is identification of phishing attempts through education and training.**

***Keywords*— phishing, cyber-attacks, platforms, SLR**

I. INTRODUCTION

Phishing is a form of social engineering that employs a number of methods to obtain someone's credit card number, email address, and other personal information.[1],[2]. According to Chiew et al. (2018)[3, the word "phishing" is derived from the word "fishing," as the operation of phishing is comparable to fishing in that the attacker "lures" the victim by using a "bait" and "fishes" for personal or confidential information from the victim.

According to Bose and Leung (2009), there are four stages to a phishing attack: (1) preparation (select target companies for phishing and look into potential system weaknesses), (2) mass broadcast (disseminate phishing messages to the general public), (3) maturity (wait for victims to respond to phishing messages), and (4) account hijack (conduct identity theft to cause victims financial loss). Berghel (2006) asserts that for phishing to be successful, the following requirements must be met: To convince an unwary person to suspend their skepticism, anything must: (1) appear genuine; (2) offer itself to an appropriate target-of-opportunity; (3) meet the reasonableness requirement; and (5) clean up after the catch. Despite everything we do, the automated preventative procedures we currently use are ineffective and fast become outdated (Jensen et al., 2017). To address this need, new strategies must be employed. Managers and end users may protect themselves and their companies by following this three-step action plan, which distills the latest research on phishing avoidance into a treasure of knowledge.

In modern culture, both the demand for security and the significance of technology have increased. Cybercriminals are gaining unauthorized access to our systems through a variety of techniques. However, these cybercriminals are increasingly focusing on the "weakest link" in the security system, rather than only attacking the devices [4].

Via order to prevent the victim from realizing that it is a phishing attempt, both the phishing website and the phishing in email are designed to look as identical as possible. The phisher can view the user's login

Received: Aug. 21, 2024; received in revised form: Oct. 10,2024; accepted: Oct. 17,2024; available online: Oct. 17,2024.

**Corresponding: aagung@binus*

credentials, credit card details, and other personal information if the victim fails to recognize the email as a phishing attempt and enters their email and password. Links to websites with malware that can harm users' devices may be included in phishing emails. [6]

As more criminals utilize internet scams to steal users' personal information, awareness of phishing attacks must increase [7]. Phishing protection is becoming essential. Despite the fact that we've learned to avoid spam emails, phishing emails can look legitimate. Some of them are even specially made to deceive users. There is no simple technique to ensure that you are totally protected from phishing assaults. Cybercriminals now have a wide variety of new methods to specifically target their victims thanks to the growth of digital platforms like social media and the sophistication of phishing attacks. The best method to protect yourself against a phishing operation is to always proceed with extreme care whenever you receive a message that seeks personal information, regardless of how genuine a message may first seem. The following is the breakdown of the paper. The SLR methodology is described in Section II. Section III includes the literature on results and analysis based on the study questions set in Section II. The SLR comes to a conclusion in Section IV.

II. Perposed Methods

A thorough assessment of the literature served as the paper's approach (SLR). The publications utilized in this study were assessed using the PRISMA checklist approach. On Fig. 1, the PRISMA flowchart is depicted.

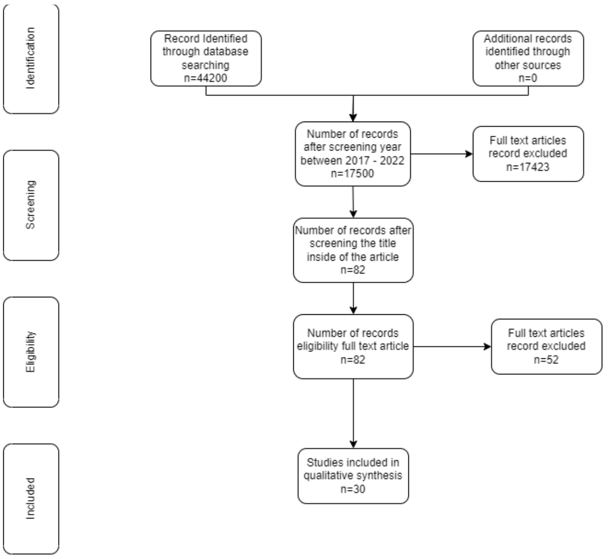
Identification
Screening
Eligibility
Included
Record Identified through database searching n=44200
Additional records identified through other sources n=0
Number of records after screening year between 2017 - 2022 n=17500
Full text articles record excluded n=17423
Number of records after screening the title inside of the article n=82
Number of records eligibility full text article n=82
Full text articles record excluded n=52
Studies included in qualitative synthesis n=30

Figure 1. PRISMA Flow Diagram

A. *Research Questions*

This systematic literature review's goal is to find information that can be utilized to avoid phishing attacks and raise people's awareness of them (based on data victim). The first thing that has to be done is to design the research questions that will be used in this study. As a result, we have designed the research question as:

RQ1: The most common environment for phishing attacks?

RQ2: What the most popular technique for phishing attacks?

RQ3: What are the most frequently suggested phishing prevention method ?

B. Search Strategy

For the next step, we do some screening with some criterias. In our analysis, English-language research publications from journals, conference proceedings, and literature reviews with domain searches for phishing avoidance are the most crucial filter criteria. Other filter criteria include the publication year of the paper, which is between 2017 and 2022, and the title of the piece, which is based on keywords. By combining all the criteria, we were able to locate the primary research.

The Google Scholar search engine show that returned 44200 pages in the initial search before applying the filter parameters when the search term "Phising Prevention" was used. 17500 papers are found after a chosen publication year between 2017 and 2022. Following the screening of 17500 papers, 17423 records are excluded. 52 papers are then eliminated from the remaining 82 papers after each one has been evaluated individually. The final results of the search were 30 publications from those processes that were retrieved from sciencedirect, researchgate, ieeexplore, itm-conferences, link.springer, ijrpr, mdpi, and iacis link from google scholar for this systematic literature review.

C. Study Selection Criteria

Research that satisfies the predetermined criteria is then excluded after collecting papers using the provided search strategy. The selected publications must satisfy all selection criteria but none of the exclusion criteria specified in Table I.

TABLE I. SELECTION CRITERIA

Selection Criteria	Exclusion Criteria
Scholarly work that has gained international acclaim	Unable to access paper
Paper about phising attack techniques	The study cited in the article

Presented in the paper are methods for phishing attack prevention	
Between 2017 and 2022 for a paper's publishing year	
Phishing attack detection in the paper	

III. Experimental ResultS

RQ1. The most common environment for phishing attacks?

According to systematic literature reviews, there are 30 paper that are divided into six different types of media used in phishing attacks. Table II classifies all media and the studies that use them:

TABLE II. ENVIRONMENT FOR PHISHING ATTACK

Environment	Number of Papers	Study Identifiers
Website	16	[3],[4],[5],[1],[6],[7],[8],[9],[2], [10],[11],[12],[13],[14],[15],[16]
Companies	10	[3],[4],[17],[8],[2],[18],[19],[20], [21],[22]
Mobile Device	7	[3],[4],[23],[8],[2],[24],[25]
Email	2	[26],[27]
Web Wallet	2	[28],[29]
Facebook	1	[30]

The website is the medium that is frequently utilized in phishing attempts, as can be seen from the table above. This is evident from the 30 studies, 16 of which exploit websites to conduct phishing assaults.

Attacks through this website are carried out by establishing an appearance identical to the actual website so that users are unaware that they have been the target of a phishing attack. For prevent phishing attacks, double-check any writing or displays on websites before opening them.

Email, web wallet, and Facebook are three forms of media phishing attempts that are rarely studied. It can be seen that only one or two papers have written about it.

Several media, including websites, businesses, and mobile applications that use the CANTINA approach and deep machine learning to prevent phishing, are used by some publications, rather than just one. One such medium is paper [1]. Paper [2] develops training programs for businesses using AI to lower the number of phishing attacks through the usage of websites, businesses, and mobile applications. One-time passwords and multi-level barrier apps are used by Paper [7] through websites, businesses, and mobile applications to prevent phishing.

RQ2. What the most popular technique for phishing attacks?

Based on information from related articles about the type of spear phishing targeted at email and the web using social engineering techniques, there are many different types of phishing attacks, including XSS, whaling, BEC, QRishing, deceptive phishing, link manipulation, MITM attacks, tab napping attacks, and more.

Three papers deal with spear phishing, four with social engineering, and one each deals with XSS, whaling, BEC, QRishing, deceptive phishing, link manipulation, MITM attack, and tab napping attacks. The highest technique is social engineering phishing (33.33%), followed by spear phishing (25%), and other techniques (8.3%).

RQ3. What are the most frequently suggested phishing prevention methods?

According to systematic literature reviews, there are 30 paper that are divided into thirteen different types suggest phishing prevention methods. Table III classifies all method and the studies that use them:

TABLE III. SUGGESTED PHISHING PREVENTION METHOD

Method	Number of Papers	Study Identifiers
Authentication	4	[9],[22],[15],[25]
Image Verification	1	[29]
Visual Website Similarity and Domain Name Based Features	1	[11]
ECDSA (for creating and confirming digital signatures) and ECIES (for message	1	[24]

encryption and decryption)		
The detection of phishing attacks education training	5	[20],[4],[6],[8],[21]
Intelligent System and Support Vector Machine	1	[5]
Distinguish between Legitimate website and Phishing website	3	[1],[28],[17]
CAPTCHA Keystroke Dynamics	1	[7]
Fuzzy Logic	1	[13]
Machine Learning	4	[14],[12],[16],[3]
CEPP Method	1	[26]
NLP Processing	1	[27]

Table 2 shows that among the 24 articles that suggest phishing prevention approaches, 5 of which propose the method for phishing prevention, the creation of a training program for phishing attack detection lessons is the method that is most frequently proposed.

Short-term and long-term learning strategies are used in Paper [20]. In the short term, it is advantageous because you can see the outcomes of the participants learning right away, and in the long term, it is advantageous because researchers can see how much the participants will retain their learning after some time. Companies are the targets for users of the suggested training strategy in Paper [2]. Employees might use AI to try and personally comprehend the kinds of phishing attacks that are anticipated to lower the amount of phishing incidences. The strategy described in Paper [5] involves sending phishing emails and offering phishing websites built using the same methods and surroundings as the actual item.

In Paper [7], a three-pillar strategy is described that is built on one-time passwords, multi-level desktop application restrictions, and behavior change. It is intended that by using this strategy, people and businesses will be better equipped to safeguard their information and lessen the harm done by phishing attempts. Paper [21] sends emails, SMS messages, or website pages that are considered phishing to disseminate anti-phishing questionnaires and carry out pretests and posttests.

IV. Conclusion

This study tries to identify the medium where phishing attacks frequently occur. 16 of the 30 publications look at online phishing attempts. Additionally, phishing attempts target businesses, mobile apps, email, web wallets, and Facebook. Phishing attacks can be classified into several categories, including XSS, whaling, BEC, QRishing, misleading phishing, link manipulation, MITM assaults, tab napping attacks, and many others. Social engineering phishing has the highest rate of success (33.33%), followed by spear phishing (25%), and other tactics (8.3%). Several techniques, including authentication, picture verification, visual website similarity, and domain name-based features—have been suggested for phishing assault detection. Distinguish between trustworthy websites and phishing websites utilizing ECDSA Keystroke Dynamics, ECIES Encryption/Decryption of Messages, Phishing Attack Educational Training Detection, Intelligent Systems and Vector Support Engines, Fuzzy Logic, Machine Learning, CEPP Method, and NLP Processing. Phishing attack education training detection is the technique that is most usually utilized. It is simpler to explain to other users how to avoid phishing using this strategy.

Other academics can utilize this information to learn more about media, types, and how to recognize phishing scams. Future recommendations for phishing detection techniques are planned with the goal of lowering the global phishing rate. Several hypotheses and factors, including the following, have been identified as having an impact on the phishing attack environment and the phishing approach. Based on our findings, we advise further research to identify the factors that influence phishing assaults the most and learn how to prevent them. Determining which attack the attacker of a different type will launch based on training and experience may help with decision-making.

References

[1] T. Doke, P. Khismatrao, V. Jambhale, and N. Marathe, “Phishing-Inspector: Detection & Prevention of Phishing Websites,” *ITM Web of Conferences*, vol. 32, p. 03004, 2020, doi: 10.1051/itmconf/20203203004.

[2] R. Alabdan, “Phishing attacks survey: Types, vectors, and technical approaches,” *Future Internet*, vol. 12, no. 10. MDPI AG, pp. 1–39, Oct. 01, 2020. doi: 10.3390/fi12100168.

[3] E. R. S. and R. Ravi, “A performance analysis of Software Defined Network based prevention on phishing attack in cyberspace using a deep machine learning with CANTINA approach (DMLCA),” *Comput Commun*, vol. 153, pp. 375–381, Mar. 2020, doi: 10.1016/j.comcom.2019.11.047.

[4] M. F. Ansari, P. K. Sharma, and B. Dash, “Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training,”

International Journal of Smart Sensor and Adhoc Network., pp. 61–72, Mar. 2022, doi: 10.47893/ijssan.2022.1221.

[5] N. Megha, K. R. Remesh Babu, and E. Sherly, "An Intelligent System for Phishing Attack Detection and Prevention," in *Proceedings of the 4th International Conference on Communication and Electronics Systems, ICCES 2019*, Jul. 2019, pp. 1577–1582. doi: 10.1109/ICCES45898.2019.9002204.

[6] University of Westminster., Institute of Electrical and Electronics Engineers, and University of Cambridge, *The 5th International Conference on Information Management (ICIM 2019) : 24-27 March, 2019, Cambridge, UK.*

[7] E. K. Alamri, A. M. Alnajim, and S. A. Alsuhibany, "Investigation of Using CAPTCHA Keystroke Dynamics to Enhance the Prevention of Phishing Attacks," *Future Internet*, vol. 14, no. 3, Mar. 2022, doi: 10.3390/fi14030082.

[8] "PREVENTION OF PHISHING ATTACKS: A THREE-PILLARED APPROACH," *Issues In Information Systems*, 2020, doi: 10.48009/2_iis_2020_1-8.

[9] E. Ulqinaku, D. Lain, and S. Capkun, "2FA-PP: 2nd factor phishing prevention," in *WiSec 2019 - Proceedings of the 2019 Conference on Security and Privacy in Wireless and Mobile Networks*, May 2019, pp. 60–71. doi: 10.1145/3317549.3323404.

[10] V. Bhavsar, A. Kadlak, and S. Sharma, "Study on Phishing Attacks," *Int J Comput Appl*, vol. 182, no. 33, pp. 27–29, Dec. 2018, doi: 10.5120/ijca2018918286.

[11] W. H. Lim, W. Foong Liew, C. Y. Lum, and S. F. Lee, "Phishing Security: Attack, Detection, and Prevention Mechanisms." [Online]. Available: www.facebook.com.

[12] *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA).*

[13] M. D. Bhagwat, P. H. Patil, and T. S. Vishawanath, "A methodical overview on detection, identification and proactive prevention of phishing websites," in *Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021*, Feb. 2021, pp. 1505–1508. doi: 10.1109/ICICV50876.2021.9388441.

[14] A. J. Tallón-Ballesteros, S. J. Fong, and R. K. K. Wong, "An empirical study on performance server analysis and URL phishing prevention to improve system management through machine learning," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2019, vol. 11113 LNCS, pp. 199–207. doi: 10.1007/978-3-030-13342-9_17.

[15] V. Muthuraman, K. Selvan, and M. Vanitha, "Detection of phishing web pages based on features vector and prevention using multi layered authentication." [Online]. Available: http://www.acadpubl.eu/hub/

[16] H. Mali, P. Chavan, A. Habib, A. Dhotre, and N. Kamble Student, "International Journal of Research Publication and Reviews Detection and Prevention of Phishing Using Machine Learning," *International Journal of Research Publication and Reviews*, vol. 2, pp. 1366–1370, 2021, [Online]. Available: http://217.102.24.235/sample.html

[17] I. National Institute of Technology (Punjab, I. D. of C. S. & E. National Institute of Technology (Punjab, Institute of Electrical and Electronics Engineers. Delhi Section, and Institute of Electrical and Electronics Engineers, *ICSCCC 2018 : International Conference on Secure Cyber Computing and Communication : December 15-17, 2018.*

[18] SCAD College of Engineering and Technology and Institute of Electrical and Electronics Engineers, *Proceedings of the 4th International Conference on Trends in Electronics and Informatics (ICOEI 2020) : 15-17, June 2020*.

[19] S. Back and R. T. Guerette, "Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks," *J Contemp Crim Justice*, vol. 37, no. 3, pp. 427–451, Aug. 2021, doi: 10.1177/10439862211001628.

[20] A. Sumner and X. Yuan, "Mitigating phishing attacks: An overview," in *ACMSE 2019 - Proceedings of the 2019 ACM Southeast Conference*, Apr. 2019, pp. 72–77. doi: 10.1145/3299815.3314437.

[21] M.-S. Hwang *et al.*, "Editor-in-Chief Publishing Editors Board of Editors PUBLISHER: Candy C." [Online]. Available: http://ijeie.jalaxy.com.tw

[22] A. O. Alsayed, A. Bilgrami, W.: Www, A. O. Alsayed, and A. L. Bilgrami, "E-Banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities Using Social Media for Collaborative Learning to enhance learners? Performance on learning View project E-banking Security View project International Journal of Emerging Technology and Advanced Engineering E-Banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities," 2008. [Online]. Available: https://www.researchgate.net/publication/315399380

[23] V. Bieger, G. J. Ramackers, and D. P. M. Kwantes, "Phishing prevention in mobile messaging platforms by the Dutch banking sector," 2021.

[24] S. Bojjagani, D. R. D. Brabin, and P. V. V. Rao, "PhishPreventer: A Secure Authentication Protocol for Prevention of Phishing Attacks in Mobile Environment with Formal Verification," in *Procedia Computer Science*, 2020, vol. 171, pp. 1110–1119. doi: 10.1016/j.procs.2020.04.119.

[25] S. Nasiri, M. T. Sharabian, and M. Aajami, "Using Combined One-Time Password for Prevention of Phishing Attacks," 2017. [Online]. Available: www.etasr.com

[26] L. Jeurissen, "E-mail phishing prevention proposal: CEPP," 2021.

[27] S. Salloum, T. Gaber, S. Vadera, and K. Shaalan, "Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey," in *Procedia CIRP*, 2021, vol. 189, pp. 19–28. doi: 10.1016/j.procs.2021.05.077.

[28] A. A. Andryukhin, "Phishing Attacks and Preventions in Blockchain Based Projects," in *Proceedings - 2019 International Conference on Engineering Technologies and Computer Science: Innovation and Application, EnT 2019*, May 2019, pp. 15–19. doi: 10.1109/EnT.2019.00008.

[29] R. Parthiban, V. Abarna, M. Banupriya, S. Keerthana, and D. Saravanan, "Web Folder Phishing Discovery and Prevention with Customer Image Verification," in *2020 International Conference on System, Computation, Automation and Networking, ICSCAN 2020*, Jul. 2020. doi: 10.1109/ICSCAN49426.2020.9262395.

[30] N. Abe, Institute of Electrical and Electronics Engineers, and IEEE Computer Society, *2018 IEEE International Conference on Big Data : proceedings : Dec 10 - Dec 13, 2018, Seattle, WA, USA.*