International Journal of Research and Applied Technology

4(1)(2024) 35-47

Journal homepage: https://ojs.unikom.ac.id/index.php/injuratech

Cybernetic Deception: Unraveling the Layers of Email Phishing Threats

Hewa Majeed Zangana[1*], Ayaz khalid Mohammed[2], Amira Bibo Sallow[3], Zina Bibo Sallow[4]

[1,3] IT Dept., Duhok Technical College, Duhok Polytechnic University, Duhok, Iraq

[2,4] Computer System Department, Ararat Technical Private Institute, Kurdistan Region – Iraq

Email: * hewa.zangana@dpu.edu.krd

Abstract. E-mail phishing, a tireless and versatile cybersecurity risk, requires a intensive examination to fortify organizational resistances. This broad survey dives into the multifaceted measurements of e-mail phishing, including mental control strategies, mechanical complexities, and real-world experiences determined from assorted case considers. The investigation of location and anticipation procedures covers a extend of commitments, tending to half breed machine learning approaches, the significance of client instruction, and the part of administrative compliance. These procedures give a significant system for organizations pointing to improve their flexibility against the energetic scene of phishing strategies. The theoretical underscores the administrative landscape's significant part in forming cybersecurity hones, advertising a organized establishment for organizations to adjust with legitimate prerequisites. Expecting future patterns and challenges, such as the integration of characteristic dialect preparing procedures and the complexities of cloud-based phishing assaults, gets to be basic for maintained cyber versatility. In conclusion, this paper serves as a comprehensive direct, enabling people and organizations with the information and methodologies required to explore the complex scene of e-mail phishing dangers. It recognizes the energetic nature of the danger scene, highlighting the progressing travel in combating computerized duplicity and invigorating preparation against the ever-evolving strategies of phishing foes.

Keywords: Cybersecurity, Email Phishing, Phishing Attacks, Threats.

1. Introduction

Within the ever-evolving scene of cybersecurity, the danger of e-mail phishing stands out as a tireless and continuously advanced risk. The predominance of phishing assaults has heightened, requiring a careful understanding of their complexities and the improvement of vigorous countermeasures [1]-[3]. This paper dives into the multifaceted domain of mail

International Journal of Research and Applied Technology

4(1)(2024) 35-47

Journal homepage: https://ojs.unikom.ac.id/index.php/injuratech

phishing, pointing to disentangle its layers and shed light on the advancing strategies utilized by cybercriminals.

The expanding advancement of phishing assaults, outlining the require for a nuanced investigation of this cyber danger scene [4]-[6]. The gravity of the circumstance, highlighting the state of the craftsmanship and future challenges in combating phishing assaults [7]-[10]. As organizations grapple with these challenges, there's a developing direness to comprehend the different sorts of mail phishing methods that foes utilize.

The important experiences into the different phishing methods, advertising a comprehensive see of the strategies utilized by cybercriminals [8]-[14]. Understanding these techniques is significant for invigorating guards and formulating successful countermeasures. Additionally, the mental measurements of phishing assaults, uncover the perplexing transaction between social designing strategies and human behavior misuse [15-17].

As organizations hook with the double challenges of innovative advancement and mental control, a comprehensive examination of the innovative angles of phishing gets to be basic [18-20]. The specialized strategies utilized by aggressors, shedding light on perspectives such as spoofing and malware dispersion [4], [5].

This paper points to synthesize these differing viewpoints into a cohesive understanding of e-mail phishing dangers, drawing on a wealthy cluster of ponders and case examinations [21]. By doing so, it looks for to prepare per users with the information required to explore the complex territory of computerized misdirection and brace resistances against the advancing strategies of phishing aggressors [22].

2. Types of Email Phising and Reviewed Works

The scene of e-mail phishing is characterized by a differing cluster of strategies utilized by cyber enemies. Understanding these different sorts is pivotal for organizations pointing to reinforce their resistances against this unavoidable risk.

2.1 Spear Phising

Skewer phishing, includes focused on assaults on particular people or organizations [1]. The aggressors fastidiously tailor their messages, frequently leveraging individual data to betray beneficiaries. This level of personalization upgrades the viability of skewer phishing, making it a strong device within the hands of cybercriminals.

2.2 Social Engineering Techniques

Building on the establishments of mental control, phishing assaults habitually utilize social designing strategies. This incorporates abusing believe, fear, or criticalness to trap people into disclosing touchy data. The significance of understanding the mental measurements behind these methods [7], [10].

2.3 Machine Learning-Aided Phishing

As innovation progresses, so do the strategies utilized by phishing aggressors. The integration of machine learning and normal dialect preparing to improve phishing e-mail discovery [3], [15]. This sort of modern approach postures a significant challenge, requiring organizations to receive similarly progressed mechanical resistances.

International Journal of Research and Applied Technology

4(1)(2024) 35-47

Journal homepage: https://ojs.unikom.ac.id/index.php/injuratech

2.4 Cloud-Based Phishing Attacks

The crossing point of cloud computing and phishing, outlining the versatility of aggressors [5]. Cloud-based mail phishing assaults, fuelled by machine and profound learning calculations, posture one-of-a-kind challenges for location and anticipation. Understanding these subtleties is imperative for organizations depending on cloud-based communication stages.

2.5 Content-Based Phishing

The present content-based phishing location strategies, emphasizing the part of analysing mail substance for danger recognizable proof [6]. This approach centres on the printed components of phishing emails, contributing to an expanded arms stockpile of discovery procedures. Table 1 show Indicates a comprehensive rundown of surveyed works on phishing.

Table 1. Comprehensive Table of Reviewed Works

Authors	Year	Work	Results
[1]	2022	Detection and Binary Classification of Spear-Phishing Emails in Organizations Using a Hybrid Machine Learning Approach.	Proposed a hybrid machine learning approach for detecting and classifying spear-phishing emails, enhancing accuracy in identifying targeted attacks.
[2]	2017	Phishing environments, techniques, and countermeasures: A survey.	Provided a comprehensive survey of phishing environments, techniques, and countermeasures, offering insights into the diverse landscape of phishing threats.
[3]	2021	Applying machine learning and natural language processing to detect phishing email.	Explored the application of machine learning and natural language processing for phishing email detection, contributing to advancements in automated threat identification.
[4]	2021	A comprehensive survey of AI-enabled phishing attacks detection techniques.	Conducted a thorough survey of AI-enabled phishing attack detection techniques, offering an overview of advancements in the field.
[5]	2023	Cloud-based email phishing attack using machine and deep learning algorithm.	Explored cloud-based email phishing attacks employing machine and deep learning algorithms, highlighting the challenges and nuances of such attacks.
[6]	2017	A content-based phishing email detection method.	Proposed a content-based phishing email detection method, emphasizing the analysis of email content for threat identification.

International Journal of Research and Applied Technology

4(1)(2024) 35-47

Journal homepage: https://ojs.unikom.ac.id/index.php/injuratech

Authors	Year	Work	Results
[7]	2019	How persuasive is a phishing email? A phishing game for phishing awareness.	Introduced a phishing game to evaluate the persuasiveness of phishing emails, contributing to phishing awareness and understanding user responses.
[8]	2020	Applicability of machine learning in spam and phishing email filtering: review and approaches.	Investigated the applicability of machine learning in spam and phishing email filtering, providing a comprehensive review and analysis of existing approaches.
[9]	2017	Fighting against phishing attacks: state of the art and future challenges.	Examined the state of the art in fighting phishing attacks and identified future challenges, contributing to the understanding of the evolving threat landscape.
[10]	2021	The Phishing Email Suspicion Test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection.	Introduced the Phishing Email Suspicion Test (PEST) to evaluate the cognitive mechanisms involved in phishing detection, enhancing understanding of human factors in threat perception.
[11]	2018	A machine learning approach towards phishing email detection.	Proposed a machine learning approach for phishing email detection, contributing to the development of automated methods to identify and combat phishing threats.
[12]	2019	A comprehensive survey for intelligent spam email detection.	Conducted a comprehensive survey on intelligent spam email detection, offering insights into the state of the art in spam detection techniques.
[13]	2020	LSTM based phishing detection for big email data.	Introduced an LSTM-based phishing detection method tailored for big email data, contributing to the application of deep learning in large-scale threat identification.
[14]	2019	Put your warning where your link is: Improving and evaluating email phishing warnings.	Explored the placement of warnings in email phishing scenarios, aiming to improve and evaluate the effectiveness of phishing warnings.
[15]	2019	Machine learning based phishing detection from URLs.	Investigated machine learning-based phishing detection focusing on URLs, providing insights into the application of machine learning in identifying phishing URLs.
[16]	2021	Phishing email detection using natural language processing techniques: a literature survey.	Conducted a literature survey on phishing email detection using natural language processing techniques, contributing to the

International Journal of Research and Applied Technology

4(1)(2024) 35-47

Journal homepage: https://ojs.unikom.ac.id/index.php/injuratech

Authors	Year	Work	Results
			understanding of linguistic analysis in threat identification.
[17]	2022	A systematic literature review on phishing email detection using natural language processing techniques.	Presented a systematic literature review on phishing email detection using natural language processing techniques, offering insights into the state of research in this area.
[18]	2021	Phishing website detection using machine learning and deep learning techniques.	Explored the use of machine learning and deep learning techniques for phishing website detection, contributing to advancements in identifying deceptive websites.
[19]	2017	Email phishing detection and prevention by using data mining techniques.	Investigated email phishing detection and prevention using data mining techniques, providing insights into leveraging data mining for identifying phishing threats.
[20]	2019	Training to detect phishing emails: Effects of the frequency of experienced phishing emails.	Explored the effects of training on detecting phishing emails, considering the frequency of exposure to phishing emails and its impact on detection capabilities.
[21]	2020	Efficient deep learning techniques for the detection of phishing websites.	Investigated efficient deep learning techniques for the detection of phishing websites, contributing to advancements in identifying deceptive online platforms.
[22]	2021	Phishing email strategies: understanding cybercriminals' strategies of crafting phishing emails.	Explored cybercriminals' strategies in crafting phishing emails, enhancing understanding of the tactics employed in email phishing attacks.
[23]	2021	Phishing email detection using persuasion cues.	Explored phishing email detection using persuasion cues, emphasizing the role of psychological cues in identifying deceptive emails.
[24]	2023	Domain-Independent Deception: A New Taxonomy and Linguistic Analysis.	Introduced a domain-independent deception taxonomy and linguistic analysis, contributing to the understanding of linguistic patterns in deceptive communication.
[25]	2020	How experts detect phishing scam emails.	Explored the methods used by experts in detecting phishing scam emails, providing insights into expert strategies for identifying deceptive communications.

International Journal of Research and Applied Technology

4(1)(2024) 35-47

Journal homepage: https://ojs.unikom.ac.id/index.php/injuratech

Authors	Year	Work	Results
[26]	2020	Phishing web site detection using diverse machine learning algorithms.	Investigated phishing website detection using diverse machine learning algorithms, contributing to the exploration of varied techniques in identifying deceptive websites.

This area lights up the multifaceted nature of mail phishing, including focused on assaults, mental control, innovative modernity, and different content-based strategies. As organizations endeavor to invigorate their resistances, a comprehensive mindfulness of these phishing sorts serves as a foundational step toward successful cybersecurity.

3. Psychology Behind Phishing

The victory of mail phishing assaults frequently pivots on the shrewd misuse of human brain research. Cybercriminals adeptly use social designing strategies to control people into uncovering touchy data. Understanding the mental measurements of phishing is foremost in creating successful countermeasures.

3.1 Social Engineering Tactics

Phishing aggressors abuse a extend of social designing strategies, as explained [7], [10]. By preying on feelings such as believe, fear, or direness, these aggressors make scenarios that provoke people to act quickly without due investigation. A more profound comprehension of these strategies is basic for people and organizations to recognize and stand up to control endeavors.

3.2 Phishing Game for Awareness

The presents a novel approach to understanding the convincingness of phishing emails through a phishing amusement [7]. This inventive strategy gives experiences into how people see and react to phishing endeavors, contributing to the plan of more compelling mindfulness campaigns.

3.3 Cognitive Mechanisms of Phishing Detection

The presents the Phishing Mail Doubt Test (Bug), a lab-based errand that assesses the cognitive components included in phishing discovery [7]. This inquiries about sheds light on the cognitive process's people utilizes when evaluating the authenticity of emails, giving important bits of knowledge for improving client mindfulness and preparing.

Understanding the mental underpinnings of phishing isn't as it were approximately recognizing manipulative strategies but moreover around engaging people with the abilities to fundamentally evaluate and confirm the authenticity of advanced communications. As the fight against phishing expands past innovative resistances, developing a security-conscious mentality gets to be a pivotal component within the progressing endeavors to obstruct cyber dangers.

4. Technological Aspects

E-mail phishing isn't as it were a mental diversion but moreover a specialized challenge that requests a nuanced understanding of the strategies utilized by assailants. This area digs into

International Journal of Research and Applied Technology

4(1)(2024) 35-47

Journal homepage: https://ojs.unikom.ac.id/index.php/injuratech

the innovative perspectives of phishing, shedding light on the complicated strategies and instruments utilized by cyber foes.

4.1 Spoofing and Malware Distribution

The give important experiences into the specialized strategies of phishing, emphasizing the predominance of spoofing and malware dissemination [4]. Spoofing includes making beguiling emails that show up authentic, whereas malware conveyance abuses these emails to spread malevolent program. A comprehensive understanding of these strategies is vital for organizations pointing to brace their protections.

4.2 Cloud-Based Phishing Attacks

Within the modern risk scene, highlight the development of cloud-based mail phishing assaults. These assaults use cloud foundation, combining machine and profound learning calculations to improve their modernity [5]. The crossing point of cloud computing and phishing presents modern challenges in discovery and avoidance, requesting progressed cybersecurity measures.

As organizations explore the advancing scene of innovative dangers, it gets to be basic to receive cutting-edge guards. Bits of knowledge from assist emphasize the significance of remaining side by side of the most recent devices and strategies utilized by aggressors [8], [22]. By understanding the mechanical complexities of e-mail phishing, organizations can support their guards and proactively relieve the dangers postured by these cyber dangers.

5. Case Studies

E-mail phishing dangers show in different and complex ways, and a comprehensive understanding of real-world case ponders is vital for invigorating protections. Analyzing outstanding occurrences gives bits of knowledge into the strategies utilized, the effect on people or organizations, and viable countermeasures. This segment presents select case thinks about, shedding light on the multifaceted nature of e-mail phishing assaults.

5.1 Example 1: Exploiting Content-Based Phishing

One case ponders, highlights a modern content-based phishing assault [6]. The aggressors adeptly controlled e-mail substance, avoiding conventional discovery strategies. Analyzing this occurrence uncovers the significance of expanding protections to envelop nuanced substance investigation strategies. A give bit of knowledge into a domain-independent double-dealing case, underlining the require for a wide understanding of etymological designs abused by aggressors [8], [22].

5.2 Example 2: Cloud-Based Email Phishing

In another occasion, exhibit a cloud-based mail phishing assault utilizing machine and profound learning calculations [5]. This case think about underscores the advancing nature of phishing strategies, requiring organizations to improve their location capabilities in cloud situations. The occurrence prompts a reevaluation of security measures, emphasizing the require for versatile cybersecurity procedures.

International Journal of Research and Applied Technology

4(1)(2024) 35-47

Journal homepage: https://ojs.unikom.ac.id/index.php/injuratech

5.3 Lessons Learned

Summarizing lessons from this case ponders, emphasize the energetic and diligent nature of phishing dangers. Common subjects incorporate the significance of proactive cybersecurity measures, ceaseless adjustment to advancing strategies, and the require for a multi-faceted defense technique. These lessons serve as vital experiences for organizations pointing to fortify their versatility against the ever-evolving scene of e-mail phishing assaults [8], [22].

By dismembering real-world cases, organizations can gather noteworthy insights, brace guards against particular strategies, and cultivate a proactive cybersecurity culture that expects and mitigates the effect of phishing dangers.

6. Detection and Prevention Strategies

As the advancement of e-mail phishing assaults proceeds to advance, organizations must send vigorous procedures for convenient discovery and avoidance. This segment investigates current innovations and best hones pointed at recognizing and obstructing phishing endeavors, drawing bits of knowledge from later investigate and down to earth applications.

6.1 Technological Detection Methods

The advocate for a crossover machine learning approach within the discovery and double classification of spear-phishing emails [1]. This highlights the part of progressed calculations in observing unobtrusive designs characteristic of noxious expectation. Furthermore, [13] proposes a Long Short-Term Memory (LSTM)-based phishing discovery instrument, displaying the utilization of profound learning for improved precision, particularly when managing with expansive e-mail datasets.

6.2 User Education and Awareness

Compelling avoidance procedures expand past innovation to incorporate client instruction and mindfulness campaigns. the centrality of preparing programs that improve users' capacity to recognize and report phishing endeavors [11]. The encourage emphasize the significance of teaching clients on how specialists identify phishing trick emails, engaging them to be careful against advancing strategies [22].

6.3 Regulatory Compliance and Standards

Compliance with cybersecurity directions and guidelines is fundamentally to a comprehensive defense procedure. Examine the administrative scene, emphasizing how adherence to build up systems can direct organizations in executing compelling phishing avoidance measures. Understanding and executing these benchmarks contribute to all-encompassing approach in shielding against e-mail phishing dangers [26].

6.4 Emerging Technologies

Later progressions, dive into the crossing point of characteristic dialect handling methods and phishing mail discovery [17]. By leveraging etymological investigation and machine learning, organizations can reinforce their resistances against progressively advanced phishing endeavors. Remaining side by side of such developing advances is fundamental for a proactive cybersecurity pose.

In concert, these location and avoidance methodologies emphasize the significance of a multi-layered approach. Combining mechanical arrangements, client instruction,

International Journal of Research and Applied Technology

4(1)(2024) 35-47

Journal homepage: https://ojs.unikom.ac.id/index.php/injuratech

administrative compliance, and rising innovations prepares organizations with a comprehensive toolkit to relieve the dangers postured by e-mail phishing dangers.

7. User Education and Awareness

Recognizing the significant part of people within the defense against e-mail phishing dangers, this area digs into the centrality of client instruction and mindfulness campaigns. By cultivating a security-conscious culture and preparing clients with the information to recognize and react to phishing endeavors, organizations can brace the human layer of their cybersecurity protections.

7.1 Importance of Phishing Awareness

Building on the discoveries, it is clear that educated clients shape a basic line of defense against phishing assaults [11]. Preparing programs and mindfulness activities play a significant part in upgrading users' capacity to observe suspicious emails, lessening the probability of falling casualty to tricky strategies.

7.2 Phishing Game for Awareness

The imaginative approach through a phishing diversion includes an intelligently measurement to mindfulness campaigns [7]. This gamified strategy not as it were gages users' helplessness to phishing but too serves as a lock in instructive apparatus, strengthening the lessons learned in a commonsense setting.

7.3 Cognitive Mechanisms of Phishing Detection

The understanding of cognitive instruments included in phishing location [10]. The Phishing Mail Doubt Test (Bother) presents a lab-based errand that assesses users' cognitive forms when evaluating the authenticity of emails. Bits of knowledge from this investigate help in fitting mindfulness programs to adjust with users' characteristic cognitive inclinations.

7.4 Continuous Training and Adaptation

Investigation of how specialists identify phishing trick emails highlights the energetic nature of phishing strategies [25]. Ceaseless preparing and adjustment ended up basic in this setting, guaranteeing that clients stay side by side of advancing dangers and are prepared with the abilities to recognize and react successfully.

By emphasizing client instruction and mindfulness activities, organizations can make a flexible human firewall. Clients who are well-informed, routinely prepared, and cognizant of phishing strategies contribute essentially to the generally cybersecurity pose, relieving dangers and improving the organization's capacity to upset e-mail phishing dangers.

8. Regulatory Landscape

Within the domain of e-mail phishing, the administrative scene plays a significant part in forming and directing cybersecurity hones. This segment investigates the existing cybersecurity controls and benchmarks, highlighting their significance in tending to mail phishing dangers and cultivating a secure computerized environment.

8.1 Overview of Cybersecurity Regulations

The significance of understanding and complying with cybersecurity controls [26]. An outline of these directions gives organizations with an establishment for building up vigorous

International Journal of Research and Applied Technology

4(1)(2024) 35-47

Journal homepage: https://ojs.unikom.ac.id/index.php/injuratech

cybersecurity arrangements and hones. Compliance not as it were mitigating legitimate dangers but moreover contributes to a comprehensive defense against mail phishing.

8.2 Adherence to Standards

Compliance with built up cybersecurity benchmarks serves as a benchmark for organizations pointing to reinforce their protections against mail phishing assaults. Understanding and following to these benchmarks, gives an organized system for actualizing preventive measures and reacting to occurrences successfully [26].

8.3 Role of Regulations in Phishing Prevention

The administrative scene isn't inactive, and as phishing strategies advance, so do directions. Understanding how directions address mail phishing dangers, empowers organizations to adjust their cybersecurity hones with lawful prerequisites. This arrangement contributes to a proactive and versatile approach to phishing anticipation [26].

8.4 Challenges and Future Considerations

Whereas directions play a vital part, the challenges in battling against phishing assaults [9]. This incorporates the require for progressing upgrades to directions to keep pace with developing dangers. As the administrative scene advances, organizations must expect future contemplations and adjust their procedures in like manner.

Exploring the administrative scene is necessarily to a comprehensive approach in tending to mail phishing dangers. By understanding, following to, and expecting changes in cybersecurity controls, organizations can construct a versatile establishment that adjusts with legitimate necessities and proactively mitigates the dangers postured by phishing assaults.

9. Future Trends and Challenges

The ever-evolving scene of e-mail phishing requests a forward-looking viewpoint to expect rising patterns and challenges. This segment investigates the direction of phishing assaults, looking at potential improvements and obstacles that organizations may experience within the future.

9.1 Emerging Trends in Phishing Attacks

The highlighting the nonstop advancement of phishing strategies [17], [23]. This incorporates the integration of characteristic dialect preparing procedures, showing a move toward more advanced and context-aware assaults. Organizations must be watchful and versatile to counter these rising patterns viably.

9.2 Anticipated Challenges

As phishing assaults ended up more modern, the have to be expect challenges in cloud-based e-mail phishing [5]. The crossing point of cloud computing and phishing presents one-of-a-kind complexities, requiring organizations to create methodologies to moderate the dangers related with assaults in cloud situations.

9.3 Technological Advancements

The appropriateness of machine learning in spam and phishing e-mail sifting [8]. Expecting mechanical headways in discovery strategies gets to be pivotal as aggressors use cutting-edge

International Journal of Research and Applied Technology

4(1)(2024) 35-47

Journal homepage: https://ojs.unikom.ac.id/index.php/injuratech

instruments. Organizations have to be stay ahead in receiving and adjusting progressed innovations to preserve viable resistances.

9.4 Human-Centric Considerations

Whereas innovative progressions are significant, the human component remains a central point in future challenges. Understanding the cognitive components included in phishing discovery will be ended up progressively critical [10]. Future techniques must include client instruction and mindfulness programs that advance in couple with developing phishing strategies.

As organizations chart their course within the confront of advancing dangers, recognizing these future patterns and challenges is foremost. Proactive measures, mechanical advancements, and human-centric techniques will be indispensably in exploring the complex scene of e-mail phishing dangers and keeping up vigorous cybersecurity protections.

10. Conclusion

Within the tireless interest of cyber versatility, this paper has unraveled the layers of e-mail phishing dangers, diving into the complexities, strategies, and countermeasures related with this inescapable cyber risk. Drawing on a riches of investigate and case ponders, it has enlightened the multifaceted nature of phishing assaults and given experiences to invigorate guards against advancing strategies.

From the mental measurements investigated [7], [10] to the mechanical complexities talked about by Basit [4], [5], each aspect of e-mail phishing has been dismembered. Case ponders, such as those highlighted by [6], and [24], have served as commonsense lessons, emphasizing the energetic and versatile nature of phishing dangers.

Location and anticipation techniques, enveloping innovative progressions, client instruction, and administrative compliance, have been point by point based on the commitments of [1], [11], and [26]. The administrative scene has been investigated as a directing drive-in forming cybersecurity practices.

Expecting the longer-term patterns and challenges, as examined by [17], [5], and [8], is indispensably to the progressing fight against phishing assaults. Recognizing the significance of both mechanical progressions and human-centric contemplations is foremost for maintained cyber versatility.

In conclusion, the battle against mail phishing dangers is an ever-evolving travel. This paper serves as a comprehensive direct, preparing organizations and people with the information and methodologies required to explore the complex scene of computerized misdirection. As we see ahead, the lessons learned from the past and show will without a doubt shape a more secure and flexible future within the confront of advancing mail phishing dangers.

References

[1] Akinwale, P. F., & Jahankhani, H. (2022). Detection and Binary Classification of Spear-Phishing Emails in Organizations Using a Hybrid Machine Learning Approach. In Artificial Intelligence in Cyber Security: Impact and Implications: Security Challenges, Technical and Ethical Issues, Forensic Investigative Challenges (pp. 215-252). Cham: Springer International Publishing.

[2] Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. Computers & Security, 68, 160-196.

[3] Alhogail, A., & Alsabih, A. (2021). Applying machine learning and natural language processing to detect phishing email. Computers & Security, 110, 102414.

[4] Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommunication Systems, 76, 139-154.

[5] Butt, U. A., Amin, R., Aldabbas, H., Mohan, S., Alouffi, B., & Ahmadian, A. (2023). Cloud-based email phishing attack using machine and deep learning algorithm. Complex & Intelligent Systems, 9(3), 3043-3070.

[6] Che, H., Liu, Q., Zou, L., Yang, H., Zhou, D., & Yu, F. (2017, July). A content-based phishing email detection method. In 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C) (pp. 415-422). IEEE.

[7] Fatima, R., Yasin, A., Liu, L., & Wang, J. (2019). How persuasive is a phishing email? A phishing game for phishing awareness. Journal of Computer Security, 27(6), 581-612.

[8] Gangavarapu, T., Jaidhar, C. D., & Chanduka, B. (2020). Applicability of machine learning in spam and phishing email filtering: review and approaches. Artificial Intelligence Review, 53, 5019-5081.

[9] Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. Neural Computing and Applications, 28, 3629-3654.

[10] Hakim, Z. M., Ebner, N. C., Oliveira, D. S., Getz, S. J., Levin, B. E., Lin, T., ... & Wilson, R. C. (2021). The Phishing Email Suspicion Test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection. Behavior research methods, 53, 1342-1352.

[11] Harikrishnan, N. B., Vinayakumar, R., & Soman, K. P. (2018, March). A machine learning approach towards phishing email detection. In Proceedings of the Anti-Phishing Pilot at ACM International Workshop on Security and Privacy Analytics (IWSPA AP) (Vol. 2013, pp. 455-468).

[12] Karim, A., Azam, S., Shanmugam, B., Kannoorpatti, K., & Alazab, M. (2019). A comprehensive survey for intelligent spam email detection. IEEE Access, 7, 168261-168295.

[13] Li, Q., Cheng, M., Wang, J., & Sun, B. (2020). LSTM based phishing detection for big email data. IEEE transactions on big data, 8(1), 278-288.

[14] Petelka, J., Zou, Y., & Schaub, F. (2019, May). Put your warning where your link is: Improving and evaluating email phishing warnings. In Proceedings of the 2019 CHI conference on human factors in computing systems (pp. 1-15).

[15] Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. Expert Systems with Applications, 117, 345-357.

[16] Salloum, S., Gaber, T., Vadera, S., & Shaalan, K. (2021). Phishing email detection using natural language processing techniques: a literature survey. Procedia Computer Science, 189, 19-28.

[17] Salloum, S., Gaber, T., Vadera, S., & Shaalan, K. (2022). A systematic literature review on phishing email detection using natural language processing techniques. IEEE Access, 10, 65703-65727.

[18] Selvakumari, M., Sowjanya, M., Das, S., & Padmavathi, S. (2021, May). Phishing website detection using machine learning and deep learning techniques. In Journal of Physics: Conference Series (Vol. 1916, No. 1, p. 012169). IOP Publishing.

[19] Şentürk, Ş., Yerli, E., & Soğukpınar, İ. (2017, October). Email phishing detection and prevention by using data mining techniques. In 2017 International Conference on Computer Science and Engineering (UBMK) (pp. 707-712). IEEE.

[20] Singh, K., Aggarwal, P., Rajivan, P., & Gonzalez, C. (2019, November). Training to detect phishing emails: Effects of the frequency of experienced phishing emails. In Proceedings of the human factors and ergonomics society annual meeting (Vol. 63, No. 1, pp. 453-457). Sage CA: Los Angeles, CA: SAGE Publications.

[21] Somesha, M., Pais, A. R., Rao, R. S., & Rathour, V. S. (2020). Efficient deep learning techniques for the detection of phishing websites. Sādhanā, 45, 1-18.

[22] Stojnic, T., Vatsalan, D., & Arachchilage, N. A. (2021). Phishing email strategies: understanding cybercriminals' strategies of crafting phishing emails. Security and privacy, 4(5), e165.

[23] Valecha, R., Mandaokar, P., & Rao, H. R. (2021). Phishing email detection using persuasion cues. IEEE transactions on Dependable and secure computing, 19(2), 747-756.

[24] Verma, R., Dershowitz, N., Zeng, V., Boumber, D., & Liu, X. (2023). Domain-Independent Deception: A New Taxonomy and Linguistic Analysis. University of California–Berkeley.

[25] Wash, R. (2020). How experts detect phishing scam emails. Proceedings of the ACM on Human-Computer Interaction, 4(CSCW2), 1-28.

[26] Zamir, A., Khan, H. U., Iqbal, T., Yousaf, N., Aslam, F., Anjum, A., & Hamdani, M. (2020). Phishing web site detection using diverse machine learning algorithms. The Electronic Library, 38(1), 65-80.