Information Horizons: AMERICAN Journal of Library And Information Science Innovation
Volume 2, Issue 6, 2024 ISSN (E): 2993-2777

Comprehensive Guide to Different Types of Attacks on Email Systems

Sumit Malik
P.G. Student, Department of CSE, Sat Kabir Institute of Technology and Management, Haryana, India

Meenakshi Arora
Assistant Professor, Department of CSE, Sat Kabir Institute of Technology and Management, Haryana, India

Rohini Sharma
Assistant Professor and Corresponding Author, GPGCW, Rohtak

Abstract. *Email systems are critical to modern communication but are increasingly targeted by cyberattacks due to the sensitive information they handle. This comprehensive guide explores the various types of attacks on email systems, including phishing, spear phishing, whaling, business email compromise (BEC), email spoofing, malware delivery, and spamming. It also delves into more sophisticated techniques like man-in-the-middle (MitM) attacks, credential harvesting, ransomware, impersonation attacks, denial of service (DoS) attacks, and email account compromise. By examining the methods and impacts of these attacks, this guide aims to enhance awareness and preparedness against potential threats. Furthermore, it outlines preventive measures, such as using strong passwords, enabling two-factor authentication (2FA), implementing email filtering, educating users, employing encryption, updating software, and monitoring email activity. Through understanding and mitigating these threats, individuals and organizations can better protect their email systems and sensitive information from cybercriminal activities.*

Keywords: *denial of service (DoS) attacks, email spoofing, Spam Mail.*

1. Introduction

An email attack is a cyberattack that leverages email as the primary vector to deliver malicious payloads, deceive recipients, or steal sensitive information. These attacks exploit the trust and familiarity of email communication, making them a prevalent and dangerous form of cybercrime [1]. Phishing is a broad term covering various types of email scams where attackers send fraudulent emails that appear to come from reputable sources. These emails often contain links to malicious websites or attachments that deliver malware. Phishing can target many recipients at once (bulk phishing) or focus on specific individuals (spear phishing). The spear phishing targets a specific individual or organization. Attackers customize their messages based on detailed research about the victim, making these emails appear highly legitimate and personalized. Spear phishing is often used to steal login credentials or deploy malware [2]. Whaling, a form of spear phishing, targets high-profile individuals within an organization, such as CEOs or CFOs. The goal is usually to steal sensitive information or authorize large financial transactions. These emails are meticulously crafted to appear as authentic communications from trusted sources.

Business Email Compromise (BEC) attacks involve attackers gaining access to or spoofing a business email account to deceive employees into making unauthorized transfers or sharing confidential information. This type of attack is highly sophisticated and often leads to significant financial losses[3]. In clone phishing, attackers replicate a legitimate email that the recipient has previously received and alter it to contain malicious links or attachments. The attacker then sends the cloned email, making it appear as a follow-up or related message[4]. Malware Distribution: Emails are used to distribute malware, either through infected attachments or links leading to malicious websites. This malware can include ransomware, spyware, trojans, and other harmful software designed to compromise the victim's device or network[5]. Credential Phishing: These attacks aim to steal login credentials by directing recipients to fake login pages that mimic legitimate websites. Once the victim enters their credentials, the attacker captures them for unauthorized use. Angler Phishing: Angler phishing utilizes social media platforms to deceive users. Attackers impersonate trusted entities or support accounts to send direct messages containing malicious links or requests for personal information. Search Engine Phishing: Cybercriminals manipulate search engine results to lead users to malicious websites designed to capture personal information or distribute malware. These sites often closely mimic legitimate ones to deceive users[6]. Phishing is a social engineering technique that leverages a variety of strategies and tactics to target system flaws and persuade end users to divulge sensitive personal information (such as an email address, username, password, or financial information), which the attacker can then use against the victim. According to this terminology's reasoning, an attacker lures the victim with "bait" before "ph-f-fishing" for their personal data.

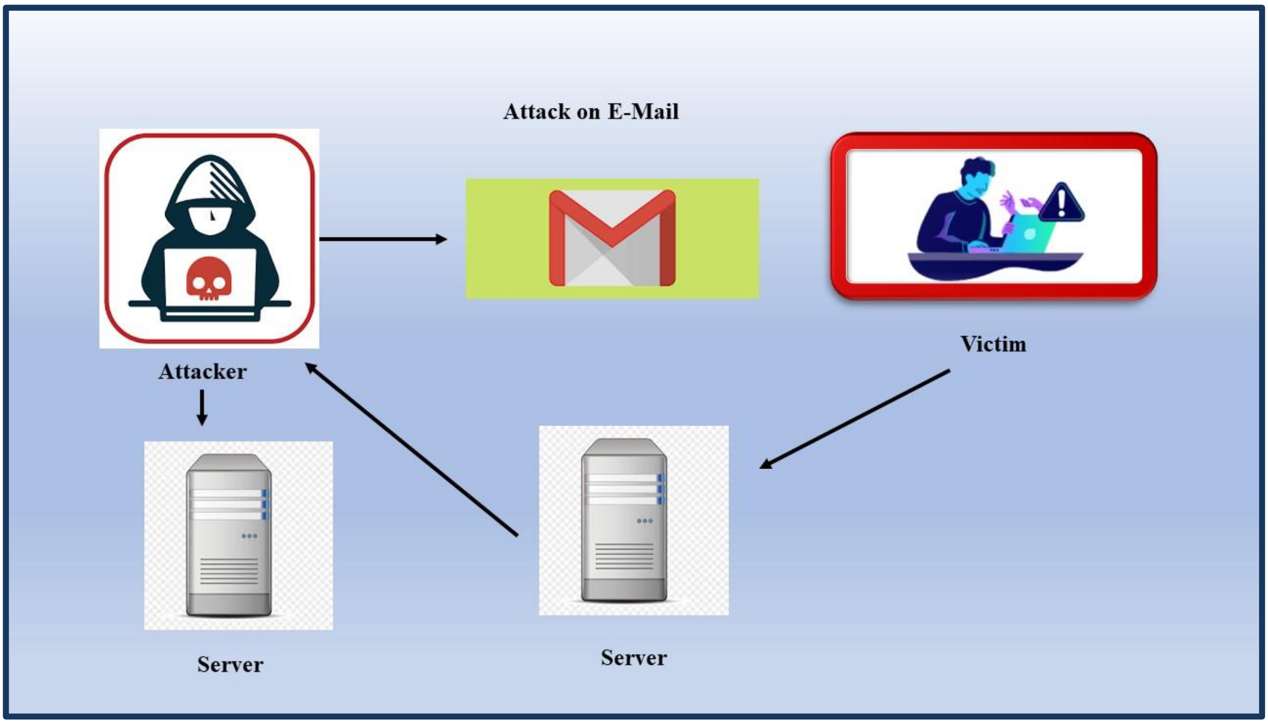

Figure 1: E-Mail Attack

2. RELATED WORK

For over two decades, researchers have been deeply interested in online deceptive attacks, and a great deal of research has been done in this area. These days, cybercriminals have been helped by the widespread use of artificial intelligence (AI) and the quick spread of online technologies such as social media, email, and smart devices for communication to create more complex deception techniques and hard-to-detect safety hazards. Published literature indicates that these attacks are significantly more skilfully exploited than what is made public, particularly when using AI technology tools [7]. It is getting harder to identify, evaluate, and control fraudulent occurrences as the cybersecurity domain gets more complicated[8]. Techno defense solutions alone can never be flawless, even though they can lessen the number of online frauds. Among other things, a deeper knowledge of the interaction between human behavioral and cognitive components towards cyberattack vulnerability is necessary for adequate security against social engineering assaults. At the same time, actions should be taken to lessen or reduce the harm that results for individuals as well as for the company [9]. Because human decision-making is the last line of defense against cyberthreats, there is a great deal of interest in determining whether and how human mental and psychological states produce neural mechanisms that can be used to reason about and possibly even identify the presence of a cyberattack [4]. Therefore, there is a special focus in research on gaze-based devices and brain-computer interfaces to help people make smart decisions by early detecting the likelihood of a cyberattack[2]. One might tackle the subject of lessening the impact of a phishing assault from various angles. Figure 2 shows different types of Phishing Media.

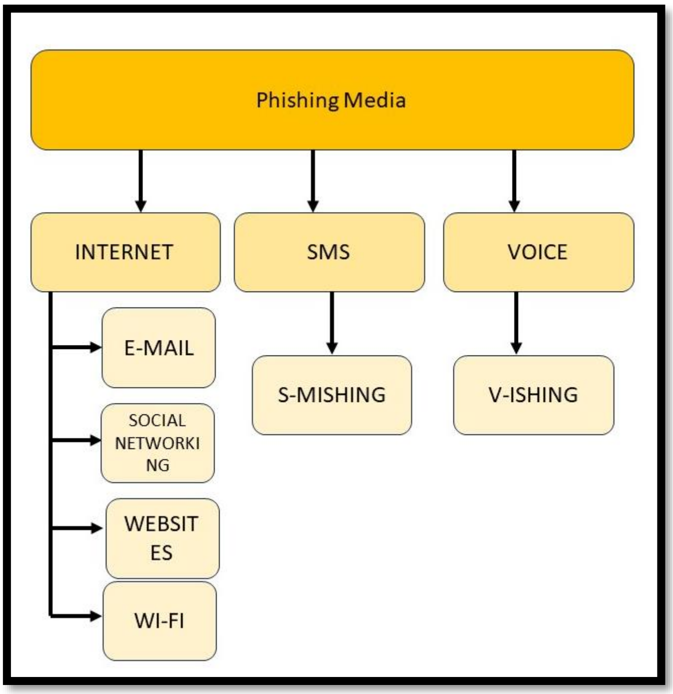

Figure 2: Types of Phishing Media

3. Phishing classification

There are a number of established classifications concerning the methods used in phishing attacks. Based on the assault target, [10] separated the phishing strategies into three groups. These divisions were general, spear, and whale phishing.

Table 1: Classification of phishing attacks Based on Existing Research (Abdillah et al. (2022)[10], Alabdan (2020)[11], Aleroud & Zhou (2017)[12], Chiew et al. (2018)[13])

Phishing Attack Type	Description	Vectors
Bulk Phishing	Generic phishing emails sent to a large number of recipients without personalization.	Email
Spear Phishing	Targeted phishing aimed at a specific individual, often involving research on the target.	Email, Social Media
Whaling	Phishing targeting high-profile individuals like CEOs or CFOs.	Email
Clone Phishing	Replication of legitimate emails with malicious links or attachments.	Email
Business Email Compromise (BEC)	Attackers compromise business email accounts to authorize fraudulent transactions.	Email
Vishing	Phishing conducted via voice calls, often involving spoofed phone numbers.	Phone Calls
Smishing	Phishing attacks delivered via SMS messages.	SMS
Angler Phishing	Using social media to deceive victims, often through fake support accounts.	Social Media
Search Engine Phishing	Manipulating search engine results to lead users to malicious websites.	Search Engines
Evil Twin	Setting up fake Wi-Fi access points to intercept data from users.	Wi-Fi Networks

Pharming	Redirecting website traffic to fraudulent sites by exploiting DNS vulnerabilities.	Web Browsers, DNS

4. SPAM MAIL

Spam mail, commonly known as junk mail, refers to unsolicited and often irrelevant messages sent over email to a large number of recipients. These messages typically include advertisements, phishing attempts, or malware delivery. Spam mail is a pervasive issue that can lead to significant problems, such as cluttered inboxes, security risks, and wasted resources.

[1] Characteristics of Spam Mail

1. **Unsolicited Messages**: Spam emails are sent without the recipient's consent, often using harvested or purchased email lists.
2. **Mass Distribution**: These emails are typically sent to a large number of recipients simultaneously.
3. **Deceptive Content**: Spam often contains misleading information, false promises, or fraudulent schemes designed to trick recipients.
4. **Malicious Attachments/Links**: Many spam emails include links to malicious websites or attachments containing malware.

[2] Types of Spam Mail

1. **Advertising Spam**: Promotes products or services, often dubious or illegal, such as fake pharmaceuticals or counterfeit goods.
2. **Phishing Spam**: Aims to deceive recipients into providing personal information, such as passwords or credit card details.
3. **Malware Spam**: Distributes malware through attachments or links, which can infect the recipient's device.
4. **Nigerian Prince Scams**: Classic scams where the sender claims to be a wealthy individual needing assistance to transfer funds, promising a large reward.
5. **Lottery Scams**: Inform recipients that they have won a large sum of money in a lottery they never entered, requiring payment of fees to claim the prize.

[3] Impact of Spam Mail

1. **Security Risks**: Spam emails can carry malware or phishing links that compromise personal and organizational security.
2. **Resource Drain**: Filtering and managing spam consumes valuable resources, including time and computing power.
3. **Financial Losses**: Falling victim to spam-related scams can result in significant financial losses for individuals and businesses.

[4] Countermeasures

1. **Spam Filters**: Email providers use filters to detect and block spam based on content, sender reputation, and other factors.
2. **User Education**: Educating users about recognizing and avoiding spam can reduce the risk of falling victim to these attacks.
3. **Legislation**: Laws like the CAN-SPAM Act in the U.S. aim to regulate commercial email and reduce spam.

Table 2: A comparison of spam mail detection techniques based on the specified references:

Criteria	**Kumar, P., & Kumar, A. (2022)**[14]	**Gupta, S., Kumaraguru, P., & Kutty, S. (2018)**[15]	**Hamed, H. M., & Faris, H. (2017)**[16]	**Ferrara, E., & Yang, Z. (2015)**[17]	**Batra, J., Bhatia, K., Sharma, R., & Bhadola, S. (2021)**[18]
Focus Area	Machine Learning Techniques for Spam Detection	Review of Machine Learning Approaches for Spam Detection	Survey on Various Spam Filtering Techniques	Measuring and Counteracting Email Spam	Development and Analysis of Spam Mail Identification Model
Techniques Analyzed	SVM, Naïve Bayes, Decision Trees, Random Forest	SVM, Naïve Bayes, Neural Networks, Ensemble Methods	Bayesian Filtering, Heuristic Methods, Blacklist/Whitelist	Statistical Methods, Machine Learning, Network Analysis	Naïve Bayes, Decision Trees, Random Forest, Gradient Boosting
Evaluation Metrics	Accuracy, Precision, Recall, F1-Score	Accuracy, Precision, Recall, F1-Score, AUC	Accuracy, False Positive Rate, False Negative Rate	Spam Ratio, Detection Accuracy, Response Time	Accuracy, Precision, Recall, F1-Score
Dataset Used	Enron Dataset, SpamAssassin Dataset	Public Spam Datasets, Proprietary Datasets	Public Spam Datasets	Public and Private Email Data	Enron Dataset, Custom Labeled Dataset
Key Findings	Random Forest showed highest accuracy; Naïve Bayes was fastest	Ensemble methods provided best balance of accuracy and speed	Bayesian filtering effective but slow; Heuristic methods faster	Machine learning improves accuracy; Statistical methods baseline	Gradient Boosting provided highest accuracy; Decision Trees were fastest
Challenges Identified	High false positives in certain techniques	Complexity of ensemble methods, high computational cost	Trade-off between speed and accuracy	Difficulty in measuring long-term effectiveness	Overfitting in complex models; need for large labeled datasets
Future Directions	Hybrid models combining multiple techniques	Improved feature selection and data preprocessing	Integration of multiple techniques for better accuracy	Real-time detection and adaptive techniques	Use of deep learning techniques; real-time spam detection models
Strengths	Comprehensive analysis of various ML	Extensive review of multiple	Broad coverage of traditional and modern techniques	Detailed analysis of effectiveness	In-depth analysis and development

	techniques	approaches		and challanges	of a new model
Limitations	Limited to certain datasets; scalability issues	High computational requirements for ensemble methods	Lack of real-time detection capabilities	Limited scope in practical application scenarios	Focus on specific models; may not generalize to all spam types

5. Recent Phishing Attack Issues and Developments

The issue of creating detection and prevention measures will not become easier or disappear with time because of the vast array of tactics and constant development of new vectors. Web-mail and software-as-a-service continue to be the most popular targets for phishing attacks, accounting for more than thirty percent of all attacks discovered in 2020. Payment industries and financial institutions follow. Since the beginning of 2020, there has also been a twenty percent increase in social media attacks [19]. It is still feasible for phishing attempts to pass undiscovered by these systems if the perpetrator takes precautions, as the majority of phishing detection techniques now in use rely on heuristics or straightforward blacklisting techniques. These could be sending emails with altered semantics, using alternative sending addresses, or deploying a botnet of compromised devices to reduce the likelihood that a phishing site would be detected. Since phishing attacks can originate from a wide variety of routes and media, anti-phishing systems are unable to identify all forms of these attacks. Since many people lack the resources or skills to adequately defend themselves, safety for everyone becomes problematic in the absence of a comprehensive answer. While this is going on, businesses can invest in the best security available. However, all it takes for a phisher to gain access to a company and increase their level of control is for one employee to disregard a warning or make a mistake. This technique is known as lateral phishing, which involves phishing employees using a valid company email address.

One of the challenges faced by researchers in this field is determining the origin of breaches in actual cyberattacks. Invasion or infection via phishing is a common tactic, but more experienced hackers (such Advanced Persistent Threats, or APT) will frequently attempt to erase as much evidence of their cybercrimes as they can during the exfiltration phase of the attack. This makes it more difficult to pinpoint the breach's origin and provides fewer details on zero-day exploits and other cutting-edge techniques these bad actors use. Like other cybercrimes, phishing is not an isolated incident. As a result, several attackers and defenders will probably use a wide range of cyberattack and defence strategies either concurrently or in concert in the future of internet security. As a result, communication and sharing of data among attackers constitutes an activity that defenders aim to restrict or stop as part of anti-phishing efforts. For instance, if a phisher manages to get into a business's network, the latter is reluctant to allow other criminals to know how their network is set up, leaving them open to further attacks. This could, however, provide some difficulties. Because cyber-security is frequently underfunded, some businesses will freeload off others rather than making the necessary investments in their own defenses. According to Hausken's concept, two attackers are pitted against two corporations. The first round of the game determines the firm's defenses, and the attackers then choose whether to launch an attack or exchange information. It was observed that corporations chose to use information sharing instead of investing in defense as the efficacy of information sharing among the firms rose. It also demonstrated how greater reliance among businesses will encourage information sharing among attackers, which will ultimately result in coordinated attacks.

Sharing data is important to attackers when attacks are expensive and the company's defenses are low-cost. The first hacker's increased notoriety could work against the second hacker by giving him or her fewer information and disadvantages. The information on sharing data in this study has significance since phishing is an infiltration technique that is occasionally used to distribute malware. As previously said, one attacker may use phishing to get access to a corporation, learn about its network, policies, and management structure, and then share that information with another attacker. The initial attacker might also be strategically positioned inside an enterprise to support an assault on a business with which the company is exchanging data by moving between and within the organizations through internal phishing using a valid company email account. In this case, using a real firm email address would be very helpful because the two companies have a track record of sharing information, which has built confidence. This brings up the primary issue of raising awareness, educating, and preventing phishing attacks. Even while this is a problem throughout the whole cyber security space, it is especially important to educate the public and staff about this particular issue since, as the examples above demonstrate, there aren't many automatic mechanisms to make up for users' ignorance or simple errors. Major concern arises from the fact that some users do not take cyber security seriously until it is too late, with roughly 50% of those polled being prepared to pay for generic cyber threat protection.

Table 3: A tabular comparison of the existing references on email phishing and related security issues

Criteria	**Verma, P.; Goyal, A.; Gigras, Y. (2020)**[20]	**Kumar, A.; Chatterjee, J.; Díaz, V.G. (2020)**[21]	**Kumar, D.; Paccagnella, R.; Murley, P.; Hennenfent, E.; Mason, J.; Bates, A.; Bailey, M. (2019)**[22]	**Shar, L.K.; Tan, H.B.K. (2018)**[23]	**Lin, T.; Capecci, D.E.; Ellis, D.M.; Rocha, H.A.; Dommaraju, S.; Oliveira, D.S.; Ebner, N.C. (2019)**[24]
Focus Area	Email Phishing Detection using NLP and Text Classification	Hybrid Approach combining SVM, NLP, and Probabilistic Neural Networks for Phishing Detection	Emerging Threats in IoT Voice Services	Defense Mechanisms Against Cross Site Scripting (XSS) Attacks	Susceptibility to Spear-Phishing Emails based on User Demographics and Email Content
Techniques Analyzed	Natural Language Processing (NLP), Text Classification	Support Vector Machine (SVM), NLP, Probabilistic Neural Network (PNN)	Voice recognition systems, Threat detection in IoT devices	Static and Dynamic Analysis, Machine Learning	Analysis of demographic factors, Spear-phishing content evaluation, User behavior studies
Evaluation Metrics	Accuracy, Precision, Recall, F1-Score	Accuracy, Precision, Recall, F1-Score	Vulnerability assessment, Detection rate, False positive/negative rates	Detection Accuracy, Response Time	Susceptibility rate, Influence of demographics on susceptibility, Email content effectiveness
Dataset Used	Public phishing email datasets	Public and private phishing email datasets	Real-world IoT device data, Voice service interaction logs	XSS attack data from public and private sources	Custom spear-phishing emails, User demographic data
Key Findings	NLP techniques	Hybrid approach	IoT voice services are	Machine learning can	Demographics significantly

	improve phishing detection accuracy	increases detection accuracy and reduces false positives	vulnerable to emerging threats; need for enhanced security measures	significantly improve XSS attack detection	affect susceptibility to spear-phishing; personalized content increases effectiveness
Challenges Identified	High computational cost of NLP, Limited by dataset variety	Complexity of integrating multiple techniques, High computational overhead	Difficulty in real-time threat detection, Need for robust security frameworks	High false positive rates in dynamic analysis	Varied susceptibility based on user demographics; difficulty in simulating real-world spear-phishing scenarios
Future Directions	Enhancing NLP models with larger datasets and advanced algorithms	Further integration of AI techniques for improved accuracy	Development of comprehensive security frameworks for IoT devices	Combining static and dynamic analysis for better accuracy	Developing adaptive spear-phishing detection mechanisms based on user behavior patterns
Strengths	Comprehensive use of NLP for text classification in phishing detection	Innovative hybrid approach, High accuracy	Focus on emerging threats in a growing field (IoT), Practical implications for security	Detailed analysis of XSS defense mechanisms	In-depth study of user susceptibility factors, Practical implications for targeted phishing prevention
Limitations	Limited to text-based phishing emails, Scalability issues	High computational requirements, Complexity in implementation	Limited scope to IoT voice services, Does not cover other IoT threat vectors	Limited to XSS attacks, High false positive rates	Focuses only on susceptibility factors, Does not provide technical countermeasures

6. CONCLUSION

Email systems are a critical communication tool but are increasingly targeted by various cyber-attacks. Understanding these threats and their implications is essential for developing robust defence mechanisms. This guide provides an overview of the major types of email attacks, their techniques, impacts, and possible countermeasures. The landscape of email-based attacks is continuously evolving, posing significant risks to individuals and organizations alike. By understanding the various types of attacks and employing a combination of technological solutions and user education, it is possible to create a more secure email communication environment. Ongoing research and development in security techniques are crucial to staying ahead of these threats.

References

1. S. B. Jayant Batra, Kirti Bhatia, Rohini Sharma, “An Overview on Machine Learning Based Spam Mail Identification Approaches,” *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 9, no. 7, pp. 8987–8993, 2021.

2. G. A. Thomopoulos, D. P. Lyras, and C. A. Fidas, “A systematic review and research challenges on phishing cyberattacks from an electroencephalography and gaze-based perspective,” *Pers. Ubiquitous Comput.*, pp. 1–22, 2024.
3. “business email compromise.” https://www.cloudflare.com/learning/email-security/business-email-compromise-bec/
4. “Clone Phishing.” https://www.proofpoint.com/us/threat-reference/clone-phishing
5. S. Peryt, J. A. Morales, W. Casey, A. Volkmann, B. Mishra, and Y. Cai, “Visualizing a malware distribution network,” in *2016 IEEE Symposium on Visualization for Cyber Security (VizSec)*, 2016, pp. 1–4.
6. N. AllahRakha, “Transformation of Crimes (Cybercrimes) in Digital Age,” *Int. J. Law Policy*, vol. 2, no. 2, 2024.
7. A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, “A comprehensive survey of AI-enabled phishing attacks detection techniques,” *Telecommun. Syst.*, vol. 76, pp. 139–154, 2021.
8. N. Kaloudi and J. Li, “The ai-based cyber threat landscape: A survey,” *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–34, 2020.
9. R. Montañez, E. Golob, and S. Xu, “Human cognition through the lens of social engineering cyberattacks,” *Front. Psychol.*, vol. 11, p. 528099, 2020.
10. R. Abdillah, Z. Shukur, M. Mohd, and T. M. Z. Murah, “Phishing classification techniques: A systematic literature review,” *IEEE Access*, vol. 10, pp. 41574–41591, 2022.
11. R. Alabdan, “Phishing attacks survey: Types, vectors, and technical approaches,” *Futur. internet*, vol. 12, no. 10, p. 168, 2020.
12. A. Aleroud and L. Zhou, “Phishing environments, techniques, and countermeasures: A survey,” *Comput. Secur.*, vol. 68, pp. 160–196, 2017.
13. K. L. Chiew, K. S. C. Yong, and C. L. Tan, “A survey of phishing attacks: Their types, vectors and technical approaches,” *Expert Syst. Appl.*, vol. 106, pp. 1–20, 2018.
14. G. Ravi Kumar, P. Murthuja, G. Anjan Babu, and K. Nagamani, “An Efficient Email Spam Detection Utilizing Machine Learning Approaches,” in *Innovative Data Communication Technologies and Application: Proceedings of ICIDCA 2021*, Springer, 2022, pp. 141–151.
15. S. Gupta, S., Kumaraguru, P., & Kutty, “pam Email Detection: A Review of Machine Learning Approaches,” *ACM Comput. Surv.*, 2018.
16. H. Hamed, H. M., & Faris, “Survey on Email Spam Filtering Techniques. Journal of Information Security.,” 2017.
17. Z. Ferrara, E., & Yang, “Measuring and Counteracting Email Spam.,” *Commun. ACM.*, 2015.
18. S. B. Jayant Batra, Kirti Bhatia, Rohini Sharma, “Development and Analysis of SPAM MAIL Identification Model,” *Int. J. Innov. Res. Sci. Eng. Technol.*, vol. 10, no. 8, pp. 11528–11535, 2021.
19. “Anti Phishing Working Group. Phishing Activity Trends Report: 4th Quater 2019. 2019.,” 2019. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf
20. P. Verma, A. Goyal, and Y. Gigras, “Email phishing: Text classification using natural language processing,” *Comput. Sci. Inf. Technol.*, vol. 1, no. 1, pp. 1–12, 2020.
21. A. Kumar, J. M. Chatterjee, and V. G. Díaz, “A novel hybrid approach of SVM combined with NLP and probabilistic neural network for email phishing,” *Int. J. Electr. Comput. Eng.*, vol. 10, no. 1, p. 486, 2020.
22. D. Kumar *et al.*, “Emerging threats in internet of things voice services,” *IEEE Secur. Priv.*, vol. 17, no. 4, pp. 18–24, 2019.

23. L. K. Shar and H. B. K. Tan, “Defending against cross-site scripting attacks,” *Computer (Long. Beach. Calif).*, vol. 45, no. 3, pp. 55–62, 2011.

24. T. Lin *et al.*, “Susceptibility to spear-phishing emails: Effects of internet user demographics and email content,” *ACM Trans. Comput. Interact.*, vol. 26, no. 5, pp. 1–28, 2019.