Enhancing Network Security: A Study on Phishing Threats and Countermeasures

A.Ilavendhan[1][0000-0001-9241-120X] and B.Nandhitha[2]

[1] Vellore Institute of Technology, Chennai, India
ilavendhana62@pec.edu
[2] Vellore Institute of Technology, Chennai, India
nandhitha.b2022@vitstudent.ac.in

Abstract. With its incredible gains in connectivity, efficiency, and convenience, the digital age has changed the world. It has, however, also created new hazards and vulnerabilities. For monetary gain, political benefit, or personal gratification, cybercriminals, hacktivists, state-sponsored actors, and other evil entities are continually trying to exploit these weaknesses. Phishing is a cyberattack strategy used by malicious individuals to trick people or organization into divulging sensitive information, such login passwords, financial information, or personal data. A typical person would not be able to tell the difference between legitimate websites and phishing websites because they both appear quite similar. As phishing techniques evolve and become increasingly sophisticated, it is crucial for individuals and organizations alike to adopt proactive strategies for prevention and mitigation. This research paper presents multiple measures on how to mitigate phishing such as machine learning models, AI data sets that consists of pattern collection using AI, NLP based techniques, and Deep learning. This abstract serves as a foundation for a comprehensive examination of the phishing phenomenon and its implications in the ever-evolving landscape of online security.

Keywords: Phishing, Network Security, Machine learning, AI, COVID-19.

1 Introduction

Cybersecurity[11] is the systematic practice of shielding systems, networks, and programs from digital threats. These threats often target sensitive information, seeking unauthorized access, alteration, or destruction. Cybersecurity measures also address potential financial extortion through ransomware and disruptions to regular business operations.. It can be divided into five different categories like Security for critical infrastructure, Security for applications, Security of networks, Security for clouds and Security for the Internet of Things (IoT) [12] . Phishing attacks can target employees working in critical infrastructure sectors, tricking them into revealing sensitive information or providing unauthorized access. Attackers can use stolen credentials to gain unauthorized access to applications, leading to data breaches or the compromise of entire systems. They may gain access to network credentials, allowing them to infiltrate and navigate within the organization's internal network. Phishers may attempt to trick users into revealing their cloud service credentials. They can be used to compromise IoT devices by tricking users into providing credentials or downloading malicious software.

Phishing serves as a technique where cybercriminals deceive individuals into revealing sensitive information, such as passwords and credit card details. This involves the impersonation of trusted entities in emails or messages. If one unsuspectingly clicks on a harmful link, it can lead to consequences like malware infecting the device or unintentional disclosure of confidential information. Understanding user behaviour and creating efficient training programmes to increase their resilience are significant areas of attention for phishing research. This entails investigating the cognitive mechanisms that make people more prone to phishing, creating instructional materials to raise awareness, and assessing the results of these programmes.

Moreover, researchers delve into the dark underbelly of the cybercriminal world, studying the economics of phishing, tracking trends in attack methodologies, and documenting real-world case studies to gain insights into the evolving nature of this threat. To counteract phishing, efforts extend to the development of robust security measures such as multi-factor authentication and email authentication standards. In sum, the continuous exploration of phishing across various dimensions remains vital in the ongoing battle to protect individuals and organizations from the perils of online deception.

A phishing scenario Fig .1 ,typically unfolds through the reception of an email purporting to originate from a reputable and trusted source, such as a financial institution or a government agency. This email often employs urgent and alarmist language, alleging a critical issue or security concern with the recipient's account or personal information. To address the purported problem, the email urges the recipient to promptly click on a hyperlink embedded within the message, ostensibly directing them to a legitimate website for resolution.

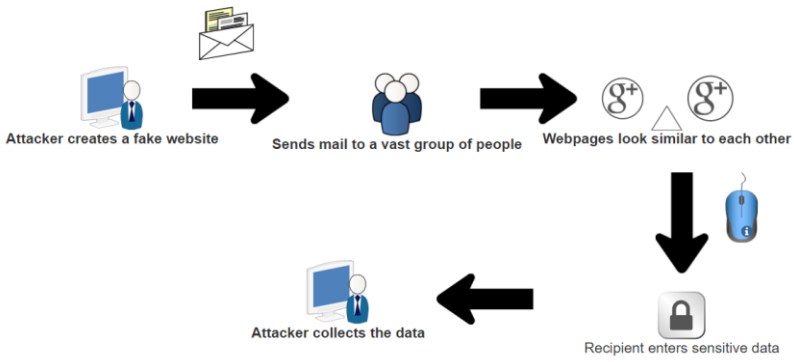

Fig. 1. The process flow of Phishing

However, careful scrutiny of the email content reveals tell-tale signs of deception, such as a generic salutation, grammatical errors, or an email sender's address that diverges from the official domain of the purported organization. These fraudulent communications, constituting phishing attempts, aim to manipulate individuals into disclosing sensitive data or login credentials, thereby facilitating

identity theft or financial fraud. In this formal context, heightened vigilance and awareness are essential in discerning and mitigating these deceptive practices.

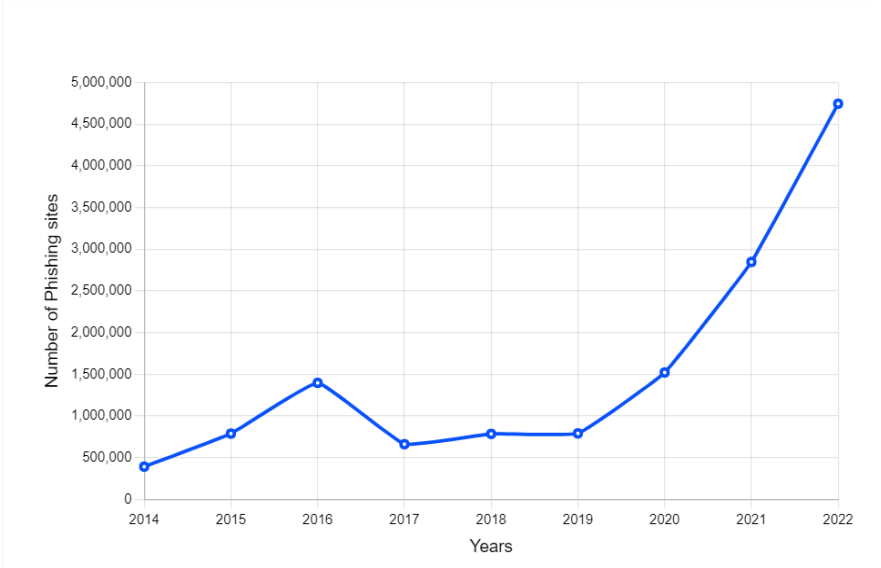

Fig. 2. Number of unique Phishing sites detected

Fig. 2 is a graph illustrating the presence of unique phishing sites over time, indicative of the growing threat posed by these malicious websites. Over the years, the number of unique phishing sites has steadily increased, reflecting the adaptability of cybercriminals and their ability to target a wide range of industries and individuals. It serves as a stark reminder of the ongoing need for robust cybersecurity measures and user awareness to combat the persistent threat of phishing attacks.

This paper delves into the various occurrences of phishing, multiple existing methods to prevent it and a proposed method to combat spear phishing efficiently.

2 Phishing Threats

There are multiple underlying causes for the occurrence of Phishing Fig .3:

- Social Engineering: Phishing primarily relies on manipulating human psychology. Attackers use tactics like fear, urgency, curiosity, and greed to deceive individuals into taking actions that compromise their security.

- Anonymity: The relative anonymity of the internet allows attackers to conceal their true identities and locations, making it challenging for law enforcement to apprehend them.

- Easy Access to Tools: Phishing tools and resources, such as phishing kits and templates, are readily available on the dark web or through illicit channels,

making it relatively simple for individuals with minimal technical skills to launch phishing attacks.

- Lack of Awareness: Many individuals and organizations lack awareness about phishing threats and effective countermeasures. This lack of knowledge increases the likelihood of falling victim to phishing attempts.

- Technological Vulnerabilities: Vulnerabilities in software, email systems, and web browsers can be exploited by attackers to enhance the effectiveness of their phishing campaigns.

- Profit Motive: Phishing attacks are often financially motivated. Attackers aim to steal valuable information, such as credit card details, login credentials, or personal data, which they can use for financial gain through identity theft or fraudulent transactions.

- Global Reach: The internet's global reach allows phishers to target victims worldwide, making it a lucrative and borderless criminal activity.

- Inadequate Security Measures: Weak or outdated cybersecurity measures in place by individuals and organizations can make them more susceptible to phishing attacks.

- Human Error: Despite technological advancements, humans remain the weakest link in cybersecurity. Even well-trained individuals can make mistakes, such as clicking on malicious links under pressure.

- Economic Factors: Economic disparities and the prospect of financial gain can motivate individuals to engage in phishing activities, particularly in regions with limited employment opportunities.

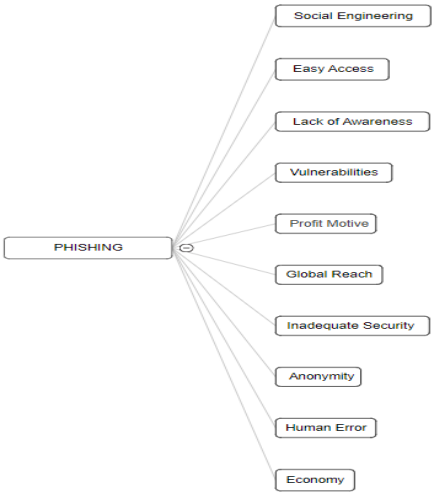

Fig. 3. Causes of Phishing

3 Various Counter Measures

A number of researchers have conducted a comprehensive study on phishing and its mitigation strategies which is discussed and projected in Table 1.

3.1 Web Phish

Chidimma et al. [1] proposed Web Phish, an end-to-end deep neural network trained using embedded raw URLs and HTML content to detect website phishing attacks. First, the proposed model automatically employs an embedding technique to extract the corresponding characters into homologous dense vectors. Then, the concatenation layer merges the URL and HTML embedding matrices. Following that, Convolutional layers are used to model its semantic dependencies.

3.2 NLP Based Technique

Sh. et al. [2] proposed a new model to extract the Arabic email content and compare it using three determinants based on neural language programming (NLP) to discover whether it is a legitimate email or a phishing email.

3.3 LSTM AI

Farheen et al. [3] offered a detection method based on artificial intelligence-based LSTM, which is a type of artificial recurrent neural network. It consists of 29 features extracted from the feature assessment module, educated through training sessions.

3.4 Spear Phish

Parvin et al. [4] built a Twitter spear phishing bot using machine learing. For the detection of phishing URLs, they used various classifiers with higher accuracy and focused on the timing to train the dataset.

3.5 Web crawler-based phishing attack detector

Nathezhtha et al. [5] formulated an algorithm to precisely detect phishing occurrence on a three-phase attack detection named Web Crawler-based Phishing Attack Detector (WC-PAD). It takes the web traffic, web content, and Uniform Resource Locator (URL) as input features. Based on these features, the classification of phishing and non-phishing websites is done.

3.6 Data Analysis

Hoheisel et al. [6] investigated how the COVID-19 pandemic influenced the phishing emails sent during the first year of the pandemic. The email content

(header data and html body, excl. attachments) is evaluated to assess how the pandemic influences the topics of phishing emails over time (peaks and trends), whether email campaigns correlate with momentous events and trends of the COVID-19 pandemic, and what hidden the content revealed.

3.7 PhizhZoo

Afroz et al. [7] proposed a phishing detection approach—PhishZoo—that uses profiles of trusted websites' appearances to detect targeted phishing attacks. It uses URLs and contents of a website to identify imitations. PhishZoo can detect current phishing sites if they look like authentic sites by matching their content against a stored profile.

3.8 Extra Trees Classifier

Arathi et al. [8] proposed a model consisting of two similar ensemble classifiers, Random Forest (RF) and Extra Trees (ET). The difference is that RF chooses an optimum split while ET chooses a split at random. The classifier model that gives the best performance metrics is selected for implementation after comparing all the models.

3.9 Deep Learning URL Detection

Dawabsheh et al. [9] devised an enhanced intelligent phishing detection tool is developed using deep learning from URLs. The system scans webpages and uses deep learning techniques to identify potentially harmful phishing content. The software is also supported with a blacklist of websites and some APIs for the reduction of time consumption as possible using a large dataset to train and test the system.

3.10 PhitKitA

Castao et al. [10] created PhiKitA, a novel dataset that contains phishing kits and also phishing websites generated using these kits. They applied MD5 hashes, fingerprints, and graph representation DOM algorithms to obtain baseline results in PhiKitA in three experiments: familiarity analysis of phishing kit samples, phishing website detection and identifying the source of a phishing website. In the familiarity analysis, evidences of different types of phishing kits and a small phishing campaign are found.

Table 1. Comparison of various countermeasures

Technique	Objective	Metrics	Advantage
WEB PHISH	Detecting phishing web pages by exploiting raw	Recall	The suggested method employs both the content found in URLs and HTML to maintain effective-

	URL and HTML characteristics		ness in countering phishing attacks.
NLP Based Technique	Detection and Analyzing Phishing Emails Using NLP Techniques	Accuracy	NLP helps detect phishing by analyzing language for inconsistencies and classifying content accurately.
LSTM AI	Prevention of Phishing attacks using AI Algorithm	Specificity	Performance is enhanced, and better classification-generated reports and findings are generated
Spear Phish	Detection Techniques Using Machine Learning Models	F1 Score	Dataset is a well feature and almost all of the model gives better accuracy.
Web Crawler-based Phishing Attack Detector.	Web Crawling based Phishing Attack Detection	Accuracy	Very effective when it comes to zero-day phishing attack Detection
Data Analysis	Evaluating Email sent during COVID-19	Datasets	Gives an extensive analytical data for future references
PHISHZOO	Phishing detection using URLs and contents of a website.	F1 Score	Has advanced algorithms and techniques for detecting phishing attempts
Extra trees classifier	Choosing the best classifier model among the datasets obtained.	Recall	Offers interpretability, efficiency, and feature importance
Deep Learning Url Detection	Using Deep Learning to mitigate Phishing attacks	Precision	Automatically extracts intricate and evolving patterns from data
PhitKitA	Use of predefined	F1 Score	Possible to relate information about

kits, MD5 hashes, fingerprints, and DOM algorithms	the attack to the phishing kit or source itself

---

Metrics Guide:

Recall = TP / (TP + FN)
Accuracy = (TP + TN) / (TP + TN + FP + FN)
Precision = TP / (TP + FP)
F1 Score = 2 x Precision x Recall / (Precision + Recall)

TP – True Positives
FP – False Positives
FN – False Negatives
TN – True Negatives

4 Proposed Model: - CYBERSENTINEL: Dynamic Spear Phishing Defense System

To overcome the vulnerabilities detected in the SPEAR PHISH technology, this section proposes a model that incorporates adaptive threat intelligence and cutting-edge technologies to optimize spear phishing detection productivity.

Cybersentinel “Fig .4” seeks to actively utilize up-to-the-minute threat intelligence feeds in a dynamic manner. By integrating these feeds, the framework is designed to remain continuously updated on emerging phishing trends, evolving attack vectors, and the latest tactics employed by malicious actors. This proposal seeks to empower organizations with the proactive capabilities necessary to detect and mitigate potential spear phishing attempts effectively, thereby bolstering their cybersecurity defences and resilience against sophisticated cyber threats.

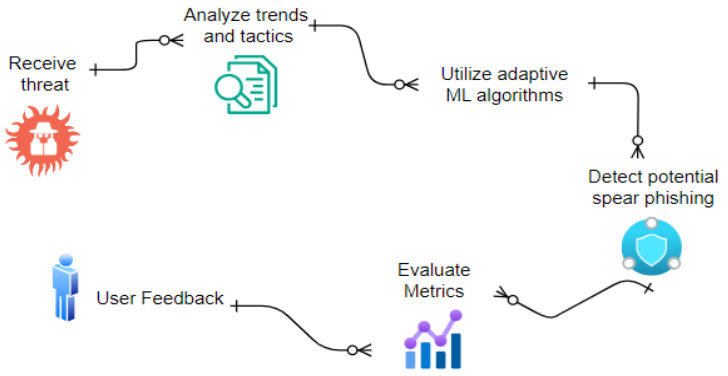

Fig. 4. Cybersentinel Model

4.1 Evalution Metrics

Detection Accuracy: An estimated experimental result could involve measuring the framework's accuracy in detecting spear phishing attempts. This could be expressed as a percentage of correctly identified phishing emails versus false positives and false negatives.

False Positive Rate: Another estimated result could focus on the false positive rate, indicating the proportion of legitimate emails incorrectly flagged as phishing attempts.

False Negative Rate: This would measure the rate at which actual phishing emails are missed by the framework, indicating its effectiveness in identifying sophisticated phishing attempts.

Response Time: An estimated experimental result could involve measuring the time it takes for the framework to detect and respond to potential spear phishing attacks, which is crucial for mitigating the impact of such threats.

4.2 Advantages over Traditional Spear Phishing Models

Dynamic Threat Intelligence:
This framework integrates real-time threat intelligence feeds. This dynamic integration enhances the framework's ability to recognize and mitigate evolving phishing threats promptly.

Linguistic flexibility:

The framework keeps a record of nuanced linguistic patterns. This sophisticated analysis helps discern subtle indicators of phishing, reducing false positives and improving the overall accuracy of the detection model.

Defensive measures:
The framework incorporates proactive defense measures to identify and mitigate potential phishing threats before they can cause harm.
This proactive stance minimizes response times, reducing the window of vulnerability and enhancing the organization's overall security posture.

Adaptive Machine Learning:
The framework utilizes adaptive machine learning, enabling continuous learning and improvement based on evolving threat landscapes.
This enhances the accuracy of spear phishing detection over time by incorporating new patterns and indicators of phishing attacks.

5 Conclusion

In conclusion, this research underscores that while phishing is a persistent threat, it is one that can be mitigated with a combination of technological solutions, user education, and proactive cybersecurity measures. The comparative analysis of various spear phishing detection models underscores the importance of employing comprehensive and integrated approaches that leverage the strengths of multiple techniques, such as machine learning, deep learning, and natural language processing, to achieve higher detection accuracy and lower false positive rates.

Moreover, by integrating Cybersentinel with spear phish detection methods we enhance defense against phishing, leveraging real-time intelligence and user training to fortify cybersecurity resilience and protect critical data.

References

[1] Opara, C., Chen, Y., & Wei, B. (2024). Look before You leap: Detecting phishing web pages by exploiting raw URL And HTML characteristics. Expert Systems with Applications, 236, 121183.

[2] Al-Yozbaky, R. S., & Alanezi, M. (2023, June). Detection and Analyzing Phishing Emails Using NLP Techniques. In 2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-6). IEEE.

[3] Ansari, M. F., Panigrahi, A., Jakka, G., Pati, A., & Bhattacharya, K. (2022, November). Prevention of Phishing attacks using AI Algorithm. In 2022 2nd Odisha International Conference on Electrical Power Engineering, Communication and Computing Technology (ODICON) (pp. 1-5). IEEE..

[4] Ripa, S. P., Islam, F., & Arifuzzaman, M. (2021, July). The emergence threat of phishing attack and the detection techniques using machine learning models. In 2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI) (pp. 1-6). IEEE..

[5] Nathezhtha, T., Sangeetha, D., & Vaidehi, V. (2019, October). WC-PAD: web crawling based phishing attack detection. In 2019 International Carnahan Conference on Security Technology (ICCST) (pp. 1-6). IEEE.

[6] Hoheisel, R., Van Capelleveen, G., Sarmah, D. K., & Junger, M. (2023). The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains. Computers & Security, 128, 103158.

[7] Afroz, S., & Greenstadt, R. (2011, September). Phishzoo: Detecting phishing websites by looking at them. In 2011 IEEE fifth international conference on semantic computing (pp. 368-375). IEEE.

[8] Anusree, A., Jose, B., Anilkumar, K., & Lee, O. T. (2021, October). Phishing Detection using Extra Trees Classifier. In 2021 5th International Conference on Information Systems and Computer Networks (ISCON) (pp. 1-6). IEEE.

[9] Dawabsheh, A., Jazzar, M., Eleyan, A., Bejaoui, T., & Popoola, S. (2022, November). An Enhanced Phishing Detection Tool Using Deep Learning From URL. In 2022 International Conference on Smart Applications, Communications and Networking (SmartNets) (pp. 1-6). IEEE.

[10] Castano, F., Fernández, E. F., Alaiz-Rodríguez, R., & Alegre, E. (2023). PhiKitA: Phishing Kit Attacks dataset for Phishing Websites Identification. IEEE Access.

[11] Kemmerer, R. A. (2003, May). Cybersecurity. In 25th International Conference on Software Engineering, 2003. Proceedings. (pp. 705-715). IEEE.

[12] Lee, C., & Fumagalli, A. (2019, April). Internet of things security-multilayered method for end to end data communications over cellular networks. In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT) (pp. 24-28). IEEE.